National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
01 - 15 Dec 2022 Vol. 09 No. 23

Table of Content

Vendor	Product	Page Number
Festo	controller_cecc-x-m1	871
	controller_cecc-x-m1-mv	871
	controller_cecc-x-m1-mv-s1	872
	controller_cecc-x-m1-y-yjkp	872
	controller_cecc-x-m1-ys-l1	872
	controller_cecc-x-m1-ys-l2	873
	controller_cmxh-st2-c5-7-diop	873
	controller_sbrd-q	873
	control_block_cpx-cec	874
	control_block_cpx-cec-c1	874
	control_block_cpx-cec-c1-v3	874
	control_block_cpx-cec-m1	875
	control_block_cpx-cec-m1-v3	875
	control_block_cpx-cec-s1-v3	875
	control_block_cpx-cmxx	876
	control_block_cpx-fec-1-ie	876
	ethernet\/ip_interface_cpx-ap-i-ep-m12	876
	ethernet\/ip_interface_cpx-ap-i-pn-m12	877
	gateway_cpx-iot	877
	integrated_drive_emca-ec-67	877
	integrated_drive_emca-ec-67-m-1te-ep	878
	motor_controller_cmmo-st-c5-1-dion	878
	motor_controller_cmmo-st-c5-1-diop	878
	motor_controller_cmmo-st-c5-1-lkp	879
	motor_controller_cmmp-as-c10-11a-p3-m0	879
	motor_controller_cmmp-as-c10-11a-p3-m3	879
	motor_controller_cmmp-as-c15-11a-p3-m3	880
	motor_controller_cmmp-as-c2-3a-m0	880
	motor_controller_cmmp-as-c2-3a-m3	880
	motor_controller_cmmp-as-c5-11a-p3-m0	881
	motor_controller_cmmp-as-c5-11a-p3-m3	881
	motor_controller_cmmp-as-c5-3a-m0	881

Vendor	Product	Page Number
mediatek	mt6753	1040
	mt6757	1040
	mt6757c	1041
	mt6757cd	1041
	mt6757ch	1041
	mt6761	1042
	mt6762	1044
	mt6763	1046
	mt6765	1046
	mt6768	1050
	mt6769	1054
	mt6771	1056
	mt6779	1057
	mt6781	1061
	mt6785	1065
	mt6789	1068
	mt6833	1073
	mt6853	1077
	mt6853t	1082
	mt6855	1083
	mt6873	1088
	mt6875	1093
	mt6877	1095
	mt6879	1100
	mt6883	1103
	mt6885	1107
	mt6889	1110
	mt6891	1113
	mt6893	1115
	mt6895	1119
	mt6983	1124
	mt7663	1127

Vendor	Product	Page Number
unisoc	t616	1322
	t618	1332
	t760	1343
	t770	1353
	t820	1363
westerndigital	my_cloud	1374
	my_cloud_dl2100	1375
	my_cloud_dl4100	1375
	my_cloud_ex2100	1376
	my_cloud_ex2_ultra	1377
	my_cloud_ex4100	1378
	my_cloud_home	1379
	my_cloud_home_duo	1379
	my_cloud_mirror_g2	1380
	my_cloud_pr2100	1380
	my_cloud_pr4100	1381
	sandisk_ibi	1382
	wd_cloud	1382
xiongmaitech	mbd6304t	1383
	nbd6808t-pl	1384
	nbd7004t-p	1385
	nbd7008t-p	1386
	nbd7016t-f-v2	1388
	nbd7024h-p	1390
	nbd7024t-p	1391
	nbd7804r-fw	1393
	nbd7804r-f\(ep\)	1394
	nbd7804r-f\(hdmi\)	1396
	nbd7804t-pl	1397
	nbd7808r-pl\(ep\)	1399
	nbd7808r-pl\(hdmi\)	1401
	nbd7808t-pl	1402

Vendor	Product	Page Number
xiongmaitech	nbd7904r-fs	1404
	nbd7904t-p	1405
	nbd7904t-pl	1407
	nbd7904t-pl-xpoe	1408
	nbd7904t-plc-xpoe	1409
	nbd7904t-q	1410
	nbd7908t-q	1412
	nbd8004r-pl\(ep\)	1413
	nbd8004r-yl\(ep\)	1415
	nbd8004t-q	1416
	nbd8008r-pl	1417
	nbd8008r-pl\(ep\)	1419
	nbd8008r-yl\(ep\)	1420
	nbd8008ra-gl	1421
	nbd8008ra-glk	1422
	nbd8008ra-ula	1423
	nbd8008ra-ulk	1424
	nbd8008ra-ul\(ep\)	1424
	nbd8008t-q	1425
	nbd8009s-ula-v2	1427
	nbd8010s-kl-v2	1428
	nbd8016r-ul	1428
	nbd8016ra-k\(ep\)	1430
	nbd8016ra-ul	1431
	nbd8016ra-ula	1432
	nbd8016ra-ulk	1432
	nbd8016ra-ul\(ep\)	1433
	nbd8016s-kl-v2	1434
	nbd8016s-ula-v2	1435
	nbd8016t-q-v2	1436
	nbd8025r-ul	1437
	nbd8032h4-p	1439

Vendor	Product	Page Number
Zyxel	atp800	1473
	usg40	1474
	usg40w	1475
	usg60	1475
	usg60w	1476
	usg_flex_100w	1477
	usg_flex_200	1477
	usg_flex_500	1478
	usg_flex_50w	1478
	usg_flex_700	1479
	vpn100	1480
	vpn1000	1480
	vpn300	1481
	vpn50	1482
Operating System		
ami	megarac_sp-x	1482
Apple	macos	1483
Arubanetworks	arubaos	1484
Asus	nas-m25_firmware	1497
BD	bodyguard_121_twins_firmware	1497
	bodyguard_323_colorvision_firmware	1498
	bodyguard_999-603_firmware	1498
	bodyguard_duo_999-903_firmware	1499
	bodyguard_epidural_999-683_firmware	1499
	bodyguard_pain_manager_999-803_firmware	1500
	bodyguard_t_999-103_firmware	1500
Brocade	fabric_operating_system	1501
Buffalo	bhr-4grv_firmware	1503
	dwr-hp-g300nh_firmware	1509
	dwr-pg_firmware	1516
	fs-600dhp_firmware	1523
	fs-g300n_firmware	1529

Vendor	Product	Page Number
Buffalo	fs-hp-g300n_firmware	1536
	fs-r600dhp_firmware	1543
	hw-450hp-zwe_firmware	1549
	wcr-300_firmware	1557
	wem-1266wp_firmware	1563
	wem-1266_firmware	1567
	wer-a54g54_firmware	1571
	wer-ag54_firmware	1577
	wer-am54g54_firmware	1584
	wer-amg54_firmware	1591
	whr-300hp_firmware	1597
	whr-300_firmware	1604
	whr-am54g54_firmware	1610
	whr-amg54_firmware	1617
	whr-ampg_firmware	1624
	whr-g300n_firmware	1630
	whr-g301n_firmware	1637
	whr-g54s-ni_firmware	1644
	whr-g54s_firmware	1650
	whr-g_firmware	1657
	whr-hp-ampg_firmware	1663
	whr-hp-g300n_firmware	1670
	whr-hp-g54_firmware	1677
	whr-hp-gn_firmware	1683
	whr-hp-g_firmware	1690
	wlae-ag300n_firmware	1697
	wli-h4-d600_firmware	1703
	wli-tx4-ag300n_firmware	1710
	wpl-05g300_firmware	1713
	wrm-d2133hp_firmware	1719
	wrm-d2133hs_firmware	1723
	ws024bf-nw_firmware	1727

Vendor	Product	Page Number
Buffalo	ws024bf_firmware	1733
	wtr-m2133hp_firmware	1740
	wtr-m2133hs_firmware	1744
	wxr-1750dhp2_firmware	1748
	wxr-1750dhp_firmware	1751
	wxr-1900dhp2_firmware	1755
	wxr-1900dhp3_firmware	1759
	wxr-1900dhp_firmware	1763
	wxr-5950ax12_firmware	1767
	wxr-6000ax12b_firmware	1770
	wxr-6000ax12s_firmware	1774
	wzr-1166dhp2_firmware	1778
	wzr-1166dhp_firmware	1782
	wzr-1750dhp2_firmware	1786
	wzr-1750dhp_firmware	1789
	wzr-300hp_firmware	1793
	wzr-450hp-cwt_firmware	1801
	wzr-450hp-ub_firmware	1808
	wzr-450hp_firmware	1815
	wzr-600dhp2_firmware	1823
	wzr-600dhp3_firmware	1830
	wzr-600dhp_firmware	1834
	wzr-900dhp2_firmware	1841
	wzr-900dhp_firmware	1845
	wzr-agl300nh_firmware	1852
	wzr-ampg144nh_firmware	1859
	wzr-ampg300nh_firmware	1865
	wzr-d1100h_firmware	1872
	wzr-g144nh_firmware	1879
	wzr-g144n_firmware	1886
	wzr-hp-ag300h_firmware	1893
	wzr-hp-g300nh_firmware	1899

Vendor	Product	Page Number
Festo	controller_cecc-x-m1-mv-s1_firmware	2498
	controller_cecc-x-m1-mv_firmware	2499
	controller_cecc-x-m1-y-yjkp_firmware	2499
	controller_cecc-x-m1-ys-l1_firmware	2499
	controller_cecc-x-m1-ys-l2_firmware	2500
	controller_cecc-x-m1_firmware	2500
	controller_cmxh-st2-c5-7-diop_firmware	2500
	controller_sbrd-q_firmware	2501
	control_block_cpx-cec-c1-v3_firmware	2501
	control_block_cpx-cec-c1_firmware	2501
	control_block_cpx-cec-m1-v3_firmware	2502
	control_block_cpx-cec-m1_firmware	2502
	control_block_cpx-cec-s1-v3_firmware	2502
	control_block_cpx-cec_firmware	2503
	control_block_cpx-cmxx_firmware	2503
	control_block_cpx-fec-1-ie_firmware	2503
	ethernet\/ip_interface_cpx-ap-i-ep-m12_firmware	2504
	ethernet\/ip_interface_cpx-ap-i-pn-m12_firmware	2504
	gateway_cpx-iot_firmware	2504
	integrated_drive_emca-ec-67-m-1te-ep_firmware	2505
	integrated_drive_emca-ec-67_firmware	2505
	motor_controller_cmmo-st-c5-1-dion_firmware	2505
	motor_controller_cmmo-st-c5-1-diop_firmware	2506
	motor_controller_cmmo-st-c5-1-lkp_firmware	2506
	motor_controller_cmmp-as-c10-11a-p3-m0_firmware	2506
	motor_controller_cmmp-as-c10-11a-p3-m3_firmware	2507

Vendor	Product	Page Number
Festo	motor_controller_cmmp-as-c15-11a-p3-m3_firmware	2507
	motor_controller_cmmp-as-c2-3a-m0_firmware	2507
	motor_controller_cmmp-as-c2-3a-m3_firmware	2508
	motor_controller_cmmp-as-c5-11a-p3-m0_firmware	2508
	motor_controller_cmmp-as-c5-11a-p3-m3_firmware	2508
	motor_controller_cmmp-as-c5-3a-m0_firmware	2509
	motor_controller_cmmp-as-c5-3a-m3_firmware	2509
	operator_unit_cdpx-x-a-s-10_firmware	2509
	operator_unit_cdpx-x-a-w-13_firmware	2510
	operator_unit_cdpx-x-a-w-4_firmware	2510
	operator_unit_cdpx-x-a-w-7_firmware	2510
	planar_surface_gantry_excm-30_firmware	2511
	planar_surface_gantry_excm-40_firmware	2511
	servo_cmmt-as-c12-11a-p3-ec-s1_firmware	2511
	servo_cmmt-as-c12-11a-p3-ep-s1_firmware	2512
	servo_cmmt-as-c12-11a-p3-mp-s1_firmware	2512
	servo_cmmt-as-c12-11a-p3-pn-s1_firmware	2512
	servo_cmmt-as-c2-11a-p3-ec-s1_firmware	2513
	servo_cmmt-as-c2-11a-p3-ep-s1_firmware	2513
	servo_cmmt-as-c2-11a-p3-mp-s1_firmware	2513
	servo_cmmt-as-c2-11a-p3-pn-s1_firmware	2514
	servo_cmmt-as-c2-3a-ec-s1_firmware	2514
	servo_cmmt-as-c2-3a-ep-s1_firmware	2514
	servo_cmmt-as-c2-3a-mp-s1_firmware	2515
	servo_cmmt-as-c2-3a-pn-s1_firmware	2515
	servo_cmmt-as-c3-11a-p3-ec-s1_firmware	2515
	servo_cmmt-as-c3-11a-p3-ep-s1_firmware	2516

Vendor	Product	Page Number
Festo	servo_cmmt-as-c3-11a-p3-mp-s1_firmware	2516
	servo_cmmt-as-c3-11a-p3-pn-s1_firmware	2516
	servo_cmmt-as-c4-3a-ec-s1_firmware	2517
	servo_cmmt-as-c4-3a-ep-s1_firmware	2517
	servo_cmmt-as-c4-3a-mp-s1_firmware	2517
	servo_cmmt-as-c4-3a-pn-s1_firmware	2518
	servo_cmmt-as-c5-11a-p3-ec-s1_firmware	2518
	servo_cmmt-as-c5-11a-p3-ep-s1_firmware	2518
	servo_cmmt-as-c5-11a-p3-mp-s1_firmware	2519
	servo_cmmt-as-c5-11a-p3-pn-s1_firmware	2519
	servo_cmmt-as-c7-11a-p3-ec-s1_firmware	2519
	servo_cmmt-as-c7-11a-p3-ep-s1_firmware	2520
	servo_cmmt-as-c7-11a-p3-mp-s1_firmware	2520
	servo_cmmt-as-c7-11a-p3-pn-s1_firmware	2520
	servo_drive_cmmt-st-c8-1c-ep-s0_firmware	2521
	servo_drive_cmmt-st-c8-1c-pn-s0_firmware	2521
	vtem-s1-27_firmware	2521
	vtem-s1-c_firmware	2522
flir	flir_ax8_firmware	2522
force1rc	discovery_wifi_u818a_hd\+_fpv_firmware	2523
Fortinet	fortios	2523
Franklinfueling	colibri_firmware	2528
fsi	fs020w_firmware	2529
	fs030w_firmware	2529
	fs040u_firmware	2530
	fs040w_firmware	2531
Google	android	2532
hornerautomation	rcc972_firmware	2636
HP	m2u75a_firmware	2637
	m2u76a_firmware	2637
	m2u77a_firmware	2637
	m2u81a_firmware	2638

Vendor	Product	Page Number
HP	m2u81b_firmware	2638
	m2u82a_firmware	2638
	m2u82b_firmware	2638
	m2u84a_firmware	2639
	m2u84b_firmware	2639
	m2u85a_firmware	2639
	m2u85b_firmware	2639
	m2u86a_firmware	2639
	m2u86b_firmware	2640
	m2u86c_firmware	2640
	m2u87a_firmware	2640
	m2u87b_firmware	2640
	m2u88b_firmware	2641
	m2u89b_firmware	2641
	m2u91a_firmware	2641
	m2u91b_firmware	2641
	m2u92a_firmware	2642
	m2u92b_firmware	2642
	m2u94a_firmware	2642
	m2u94b_firmware	2642
	pagewide_352dw_j6u57a_firmware	2643
	pagewide_377dw_j9v80a_firmware	2643
	pagewide_managed_p55250dw_j6u51b_firmware	2643
	pagewide_managed_p55250dw_j6u55a_firmware	2643
	pagewide_managed_p55250dw_j6u55b_firmware	2643
	pagewide_managed_p57750dw_j9v82a_firmware	2644
	pagewide_pro_452dn_d3q15a_firmware	2644
	pagewide_pro_452dw_d3q16a_firmware	2644
	pagewide_pro_477dn_d3q19a_firmware	2644

Vendor	Product	Page Number
HP	pagewide_pro_477dw_d3q20a_firmware	2645
	pagewide_pro_552dw_d3q17a_firmware	2645
	pagewide_pro_577dw_d3q21a_firmware	2645
	pagewide_pro_577z_k9z76a_firmware	2645
	z4a54a_firmware	2646
	z4a59a_firmware	2646
	z4a60a_firmware	2646
	z4a61a_firmware	2646
	z4a61b_firmware	2647
	z4a69a_firmware	2647
	z4a70a_firmware	2647
	z4a71a_firmware	2647
	z4a73a_firmware	2647
	z4a74a_firmware	2648
	z4b12a_firmware	2648
	z4b13a_firmware	2648
	z4b14a_firmware	2648
	z4b18a_firmware	2649
	z4b27a_firmware	2649
	z4b28a_firmware	2649
	z4b29a_firmware	2649
hpe	hf20c_firmware	2650
	hf20h_firmware	2651
	hf20_firmware	2653
	hf40c_firmware	2654
	hf40_firmware	2656
	hf60c_firmware	2658
	hf60_firmware	2659
	sf100_firmware	2661
	sf300_firmware	2662
IBM	aix	2664
	linux_on_zseries	2664

Vendor	Product	Page Number
IBM	power_system_ac922_\(8335-gtg\)_firmware	2665
	power_system_ac922_\(8335-gth\)_firmware	2665
	power_system_ac922_\(8335-gtx\)_firmware	2665
ifm	moneo_qha200_firmware	2666
	moneo_qha210_firmware	2666
Kyocera	ecosys_m2535dn_firmware	2666
	ecosys_m6526cdn_firmware	2669
	ecosys_m6526cidn_firmware	2672
	ecosys_p2135dn_firmware	2675
	ecosys_p4040dn_firmware	2678
	ecosys_p6026cdn_firmware	2680
	fs-1370dn_firmware	2683
	fs-c2026mfp_firmware	2686
	fs-c2126mfp\+_firmware	2689
	fs-c2126mfp_firmware	2692
	fs-c5250dn_firmware	2695
	ls-1035mfp_firmware	2697
	ls-1135mfp_firmware	2700
	ls-2100dn_firmware	2703
	ls-3140mfp\+_firmware	2706
	ls-3140mfp_firmware	2709
	ls-3640mfp_firmware	2712
	ls-4200dn_firmware	2714
	ls-4300dn_firmware	2717
	ls-c8600dn_firmware	2720
	ls-c8650dn_firmware	2723
	taskalfa_205c_firmware	2726
	taskalfa_206ci_firmware	2729
	taskalfa_255c_firmware	2731
	taskalfa_255_firmware	2734
	taskalfa_256ci_firmware	2737
	taskalfa_256i_firmware	2740

Vendor	Product	Page Number
Kyocera	taskalfa_3050ci_firmware	2743
	taskalfa_305_firmware	2746
	taskalfa_306i_firmware	2748
	taskalfa_3500i_firmware	2751
	taskalfa_3550ci_firmware	2754
	taskalfa_4500i_firmware	2757
	taskalfa_4550ci_firmware	2760
	taskalfa_5500i_firmware	2763
	taskalfa_5550ci_firmware	2765
	taskalfa_6500i_firmware	2768
	taskalfa_6550ci_firmware	2771
	taskalfa_7550ci_firmware	2774
	taskalfa_8000i_firmware	2777
Linux	linux_kernel	2780
Medtronic	guardian_link_2_transmitter_mmt-7730_firmware	2784
	guardian_link_2_transmitter_mmt-7731_firmware	2784
	guardian_link_2_transmitter_mmt-7738_firmware	2785
	guardian_link_2_transmitter_mmt-7775_firmware	2785
	guardian_link_3_transmitter_mmt-7810_firmware	2786
	guardian_link_3_transmitter_mmt-7811_firmware	2787
	minimed_620g_mmt-1750_firmware	2787
	minimed_630g_mmt-1715_firmware	2788
	minimed_630g_mmt-1754_firmware	2788
	minimed_630g_mmt-1755_firmware	2789
	minimed_640g_mmt-1711_firmware	2790
	minimed_640g_mmt-1712_firmware	2790
	minimed_640g_mmt-1751_firmware	2791
	minimed_640g_mmt-1752_firmware	2791

Vendor	Product	Page Number
Medtronic	minimed_670g_mmt-1740_firmware	2792
	minimed_670g_mmt-1741_firmware	2792
	minimed_670g_mmt-1742_firmware	2793
	minimed_670g_mmt-1760_firmware	2794
	minimed_670g_mmt-1761_firmware	2794
	minimed_670g_mmt-1762_firmware	2795
	minimed_670g_mmt-1780_firmware	2795
	minimed_670g_mmt-1781_firmware	2796
	minimed_670g_mmt-1782_firmware	2797
	mmt-1151_firmware	2797
	mmt-1152_firmware	2798
	mmt-1351_firmware	2798
	mmt-1352_firmware	2799
	mmt-7306_firmware	2799
Microsoft	windows	2800
Mikrotik	routeros	2805
Moxa	uc-2101-lx_firmware	2806
	uc-2102-lx_firmware	2806
	uc-2104-lx_firmware	2807
	uc-2111-lx_firmware	2807
	uc-2112-lx_firmware	2807
	uc-2114-t-lx_firmware	2808
	uc-2116-t-lx_firmware	2808
	uc-3101-t-ap-lx_firmware	2808
	uc-3101-t-eu-lx_firmware	2809
	uc-3101-t-us-lx_firmware	2809
	uc-3111-t-ap-lx-nw_firmware	2810
	uc-3111-t-ap-lx_firmware	2810
	uc-3111-t-eu-lx-nw_firmware	2810
	uc-3111-t-eu-lx_firmware	2811
	uc-3111-t-us-lx-nw_firmware	2811
	uc-3111-t-us-lx_firmware	2811

Vendor	Product	Page Number
Moxa	uc-3121-t-ap-lx_firmware	2812
	uc-3121-t-eu-lx_firmware	2812
	uc-3121-t-us-lx_firmware	2813
	uc-5101-lx_firmware	2813
	uc-5101-t-lx_firmware	2813
	uc-5102-lx_firmware	2814
	uc-5102-t-lx_firmware	2814
	uc-5111-lx_firmware	2814
	uc-5111-t-lx_firmware	2815
	uc-5112-lx_firmware	2815
	uc-5112-t-lx_firmware	2816
	uc-8112-lx_firmware	2816
	uc-8112a-me-t-lx_firmware	2817
	uc-8131-lx_firmware	2817
	uc-8132-lx_firmware	2818
	uc-8162-lx_firmware	2819
	uc-8210-t-lx-s_firmware	2820
	uc-8220-t-lx-ap-s_firmware	2820
	uc-8220-t-lx-eu-s_firmware	2820
	uc-8220-t-lx-us-s_firmware	2821
	uc-8220-t-lx_firmware	2821
	uc-8410a-lx_firmware	2821
	uc-8410a-nw-lx_firmware	2822
	uc-8410a-nw-t-lx_firmware	2822
	uc-8410a-t-lx_firmware	2823
	uc-8540-lx_firmware	2823
	uc-8540-t-ct-lx_firmware	2823
	uc-8540-t-lx_firmware	2824
	uc-8580-lx_firmware	2824
	uc-8580-q-lx_firmware	2824
	uc-8580-t-ct-lx_firmware	2825
	uc-8580-t-ct-q-lx_firmware	2825

Vendor	Product	Page Number
Moxa	uc-8580-t-lx_firmware	2826
	uc-8580-t-q-lx_firmware	2826
Ricoh	aficio_sp_4210n_firmware	2826
Samsung	exynos_firmware	2827
secu	secustation_firmware	2827
Sophos	xg_firewall_firmware	2833
telos	omnia_mpx_node_firmware	2835
telosalliance	omnia_mpx_node_firmware	2835
Tenda	a18_firmware	2836
	ac6_firmware	2836
	ax12_firmware	2837
	i21_firmware	2838
	i22_firmware	2839
	w20e_firmware	2841
	w30e_firmware	2841
	w6-s_firmware	2846
Tendacn	ac6_firmware	2847
Tp-link	re3000_firmware	2852
	tl-wr740n_firmware	2852
Trendnet	tew-820ap_firmware	2853
ui	edgemax_edgerouter_firmware	2853
unimo	udr-ja1604_firmware	2854
	udr-ja1608_firmware	2855
	udr-ja1616_firmware	2856
westerndigital	my_cloud_home_duo_firmware	2857
	my_cloud_home_firmware	2857
	my_cloud_os	2858
	sandisk_ibi_firmware	2859
xiongmaitech	mbd6304t_firmware	2859
	nbd6808t-pl_firmware	2860
	nbd7004t-p_firmware	2861
	nbd7008t-p_firmware	2861

Vendor	Product	Page Number
xiongmaitech	nbd7016t-f-v2_firmware	2862
	nbd7024h-p_firmware	2863
	nbd7024t-p_firmware	2864
	nbd7804r-fw_firmware	2865
	nbd7804r-f\(ep\)_firmware	2865
	nbd7804r-f\(hdmi\)_firmware	2866
	nbd7804t-pl_firmware	2867
	nbd7808r-pl\(ep\)_firmware	2868
	nbd7808r-pl\(hdmi\)_firmware	2869
	nbd7808t-pl_firmware	2869
	nbd7904r-fs_firmware	2870
	nbd7904t-pl-xpoe_firmware	2871
	nbd7904t-plc-xpoe_firmware	2872
	nbd7904t-pl_firmware	2873
	nbd7904t-p_firmware	2873
	nbd7904t-q_firmware	2874
	nbd7908t-q_firmware	2875
	nbd8004r-pl\(ep\)_firmware	2876
	nbd8004r-yl\(ep\)_firmware	2877
	nbd8004t-q_firmware	2877
	nbd8008r-pl\(ep\)_firmware	2878
	nbd8008r-pl_firmware	2879
	nbd8008r-yl\(ep\)_firmware	2880
	nbd8008ra-glk_firmware	2881
	nbd8008ra-gl_firmware	2881
	nbd8008ra-ula_firmware	2882
	nbd8008ra-ulk_firmware	2883
	nbd8008ra-ul\(ep\)_firmware	2884
	nbd8008t-q_firmware	2885
	nbd8009s-ula-v2_firmware	2885
	nbd8010s-kl-v2_firmware	2886
	nbd8016r-ul_firmware	2887

Vendor	Product	Page Number
xiongmaitech	nbd8016ra-k\(ep\)_firmware	2888
	nbd8016ra-ula_firmware	2889
	nbd8016ra-ulk_firmware	2889
	nbd8016ra-ul\(ep\)_firmware	2890
	nbd8016ra-ul_firmware	2891
	nbd8016s-kl-v2_firmware	2892
	nbd8016s-ula-v2_firmware	2893
	nbd8016t-q-v2_firmware	2893
	nbd8025r-ul_firmware	2894
	nbd8032h4-p_firmware	2895
	nbd8032h4-qe_firmware	2896
	nbd8032h4-q_firmware	2897
	nbd8032h4-ul_firmware	2897
	nbd8032h8-p_firmware	2898
	nbd8032h8-qe_firmware	2899
	nbd8032ra-ul-v2_firmware	2900
	nbd8064h8-p_firmware	2901
	nbd80n16ra-kl\(ep\)_firmware	2901
	nbd80n16ra-kl_firmware	2902
	nbd80s08s-kl\(ep\)_firmware	2903
	nbd80s10s-kl_firmware	2904
	nbd80s16s-kl\(ep\)_firmware	2905
	nbd80s16s-kl_firmware	2905
	nbd80x09ra-kl_firmware	2906
	nbd80x09s-kl_firmware	2907
	nbd88x09s-kl_firmware	2908
	nbd8904r-pl_firmware	2909
	nbd8904r-yl_firmware	2909
	nbd8904t-gsc-xpoe_firmware	2910
	nbd8904t-q_firmware	2911
	nbd8908r-pl_firmware	2912
	nbd8908r-yl_firmware	2913

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 2kblater					
Product: 2kb_amazon_affiliates_store					
Affected Version(s): * Up to (including) 2.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Dec-2022	6.1	Reflected Cross-Site Scripting (XSS) vulnerability in 2kb Amazon Affiliates Store plugin <=2.1.5 on WordPress. **CVE ID : CVE-2022-40968**	N/A	A-2KB-2KB_-191222/1
Vendor: activerecord_project					
Product: activerecord					
Affected Version(s): * Up to (excluding) 5.2.8.1					
Deserialization of Untrusted Data	05-Dec-2022	9.8	A possible escalation to RCE vulnerability exists when using YAML serialized columns in Active Record < 7.0.3.1, <6.1.6.1, <6.0.5.1 and <5.2.8.1 which could allow an attacker, that can manipulate data in the database (via means like SQL injection), the ability to escalate to an RCE. **CVE ID : CVE-2022-32224**	https://github.com/advisories/GHSA-3hhc-qp5v-9p2j	A-ACT-ACTI-191222/2
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.0.5.1					
Deserialization of Untrusted Data	05-Dec-2022	9.8	A possible escalation to RCE vulnerability exists when using YAML serialized columns in Active Record < 7.0.3.1, <6.1.6.1, <6.0.5.1 and	https://github.com/advisories/GHSA-3hhc-qp5v-9p2j	A-ACT-ACTI-191222/3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<5.2.8.1 which could allow an attacker, that can manipulate data in the database (via means like SQL injection), the ability to escalate to an RCE. **CVE ID : CVE-2022-32224**		
Affected Version(s): From (including) 6.1.0 Up to (excluding) 6.1.6.1					
Deserialization of Untrusted Data	05-Dec-2022	9.8	A possible escalation to RCE vulnerability exists when using YAML serialized columns in Active Record < 7.0.3.1, <6.1.6.1, <6.0.5.1 and <5.2.8.1 which could allow an attacker, that can manipulate data in the database (via means like SQL injection), the ability to escalate to an RCE. **CVE ID : CVE-2022-32224**	https://github.com/advisories/GHSA-3hhc-qp5v-9p2j	A-ACT-ACTI-191222/4
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.3.1					
Deserialization of Untrusted Data	05-Dec-2022	9.8	A possible escalation to RCE vulnerability exists when using YAML serialized columns in Active Record < 7.0.3.1, <6.1.6.1, <6.0.5.1 and <5.2.8.1 which could allow an attacker, that can manipulate data in the database (via means like SQL injection), the ability to escalate to an RCE. **CVE ID : CVE-2022-32224**	https://github.com/advisories/GHSA-3hhc-qp5v-9p2j	A-ACT-ACTI-191222/5

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: addonspress					
Product: advanced_import					
Affected Version(s): * Up to (excluding) 1.3.8					
Cross-Site Request Forgery (CSRF)	05-Dec-2022	6.5	The Advanced Import WordPress plugin before 1.3.8 does not have CSRF check when installing and activating plugins, which could allow attackers to make a logged in admin install arbitrary plugins from WordPress.org, and activate arbitrary ones from the blog via CSRF attacks **CVE ID : CVE-2022-3677**	N/A	A-ADD-ADVA-191222/6
Vendor: add_comments_project					
Product: add_comments					
Affected Version(s): * Up to (including) 1.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	The Add Comments WordPress plugin through 1.0.1 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-2022-3909**	N/A	A-ADD-ADD_-191222/7
Vendor: advanced_wp_columns_project					
Product: advanced_wp_columns					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.0.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	The Advanced WP Columns WordPress plugin through 2.0.6 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-2022-3426**	N/A	A-ADV-ADVA-191222/8
Vendor: aerocms_project					
Product: aerocms					
Affected Version(s): 0.0.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Dec-2022	4.9	AeroCMS v0.0.1 is vulnerable to SQL Injection via the delete parameter. **CVE ID : CVE-2022-46047**	N/A	A-AER-AERO-191222/9
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Dec-2022	4.8	AeroCMS v0.0.1 was discovered to contain a cross-site scripting (XSS) vulnerability via add_post.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Comments text field.	N/A	A-AER-AERO-191222/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46058		
Vendor: akeneo					
Product: product_information_management					
Affected Version(s): * Up to (excluding) 5.0.119					
Improper Control of Generation of Code ('Code Injection')	09-Dec-2022	8.8	Akeneo PIM is an open source Product Information Management (PIM). Akeneo PIM Community Edition versions before v5.0.119 and v6.0.53 allows remote authenticated users to execute arbitrary PHP code on the server by uploading a crafted image. Akeneo PIM Community Edition after the versions aforementioned provides patched Apache HTTP server configuration file, for docker setup and in documentation sample, to fix this vulnerability. Community Edition users must change their Apache HTTP server configuration accordingly to be protected. The patch for Cloud Based Akeneo PIM Services customers has been applied since 30th October 2022. Users are advised to upgrade. Users unable to upgrade may Replace any reference to `<FilesMatch \.php$>` in their apache httpd configurations	N/A	A-AKE-PROD-191222/11

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with: `<Location "/index.php">`. **CVE ID : CVE-2022-46157**		
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.0.53					
Improper Control of Generation of Code ('Code Injection')	09-Dec-2022	8.8	Akeneo PIM is an open source Product Information Management (PIM). Akeneo PIM Community Edition versions before v5.0.119 and v6.0.53 allows remote authenticated users to execute arbitrary PHP code on the server by uploading a crafted image. Akeneo PIM Community Edition after the versions aforementioned provides patched Apache HTTP server configuration file, for docker setup and in documentation sample, to fix this vulnerability. Community Edition users must change their Apache HTTP server configuration accordingly to be protected. The patch for Cloud Based Akeneo PIM Services customers has been applied since 30th October 2022. Users are advised to upgrade. Users unable to upgrade may Replace any reference to `<FilesMatch \.php$>` in their apache httpd configurations	N/A	A-AKE-PROD-191222/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with: `<Location "/index.php">`. **CVE ID : CVE-2022-46157**		
Vendor: algan					
Product: prens_student_information_system					
Affected Version(s): * Up to (excluding) 2.1.11					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-2022	9.8	Algan YazÄ±lÄ±m Prens Student Information System product has an unauthenticated SQL Injection vulnerability. **CVE ID : CVE-2022-2807**	https://www.usom.gov.tr/bildirim/tr-22-0708	A-ALG-PREN-191222/13
Authorization Bypass Through User-Controlled Key	02-Dec-2022	8.8	Algan Yaz?l?m Prens Student Information System product has an authenticated Insecure Direct Object Reference (IDOR) vulnerability. **CVE ID : CVE-2022-2808**	https://www.usom.gov.tr/bildirim/tr-22-0708	A-ALG-PREN-191222/14
Vendor: alist_project					
Product: alist					
Affected Version(s): 3.4.0					
Unrestricted Upload of File with Dangerous Type	12-Dec-2022	8.8	Alist v3.4.0 is vulnerable to File Upload. A user with only file upload permission can upload any file to any folder (even a password protected one). **CVE ID : CVE-2022-45968**	N/A	A-ALI-ALIS-191222/15
Affected Version(s): 3.5.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	5.4	Alist v3.5.1 is vulnerable to Cross Site Scripting (XSS) via the bulletin board. **CVE ID : CVE-2022-45970**	N/A	A-ALI-ALIS-191222/16
Vendor: Amazon					
Product: cloudwatch_agent					
Affected Version(s): * Up to (excluding) 1.247355					
Improper Handling of Insufficient Privileges	12-Dec-2022	6.8	A privilege escalation issue exists within the Amazon CloudWatch Agent for Windows, software for collecting metrics and logs from Amazon EC2 instances and on-premises servers, in versions up to and including v1.247354. When users trigger a repair of the Agent, a pop-up window opens with SYSTEM permissions. Users with administrative access to affected hosts may use this to create a new command prompt as NT AUTHORITY\SYSTEM. To trigger this issue, the third party must be able to access the affected host and elevate their privileges such that they're able to trigger the agent repair process. They must also be able to install the tools required to trigger the issue. This issue does not affect the	https://github.com/aws/amazon-cloudwatch-agent/security/advisories/GHSA-j8x2-2m5w-j939, https://github.com/aws/amazon-cloudwatch-agent/commit/6119858864c317ff26f41f576c169148d1250837#diff-76ed074a9305c04054cdebb9e9aad2d818052b07091de1f20cad0bbac34ffb52	A-AMA-CLOU-191222/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CloudWatch Agent for macOS or Linux. Agent users should upgrade to version 1.247355 of the CloudWatch Agent to address this issue. There is no recommended work around. Affected users must update the installed version of the CloudWatch Agent to address this issue. **CVE ID : CVE-2022-23511**		
Vendor: amentotech					
Product: workreap					
Affected Version(s): * Up to (excluding) 2.6.3					
Authorization Bypass Through User-Controlled Key	05-Dec-2022	7.5	The Workreap WordPress theme before 2.6.3 has a vulnerability with the notifications feature as it's possible to read any user's notification (employer or freelancer) as the notification ID is brute-forceable. **CVE ID : CVE-2022-3846**	N/A	A-AME-WORK-191222/18
Vendor: antihacker_project					
Product: antihacker					
Affected Version(s): * Up to (excluding) 4.20					
Cross-Site Request Forgery (CSRF)	12-Dec-2022	6.5	The Disable Json API, Login Lockdown, XMLRPC, Pingback, Stop User Enumeration Anti Hacker Scan WordPress plugin before 4.20 does not have proper authorisation and CSRF in an AJAX action,	N/A	A-ANT-ANTI-191222/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowing any authenticated users, such as subscriber to call it and install and activate arbitrary plugins from wordpress.org **CVE ID : CVE-2022-3880**		
Vendor: Apache					
Product: camel					
Affected Version(s): 3.19.0					
N/A	05-Dec-2022	9.8	The camel-ldap component allows LDAP Injection when using the filter option. Users are recommended to either move to the Camel-Spring-Ldap component (which is not affected) or upgrade to 3.14.6 or 3.18.4. **CVE ID : CVE-2022-45046**	https://camel.apache.org/security/CVE-2022-45046.html	A-APA-CAME-191222/20
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.14.6					
N/A	05-Dec-2022	9.8	The camel-ldap component allows LDAP Injection when using the filter option. Users are recommended to either move to the Camel-Spring-Ldap component (which is not affected) or upgrade to 3.14.6 or 3.18.4. **CVE ID : CVE-2022-45046**	https://camel.apache.org/security/CVE-2022-45046.html	A-APA-CAME-191222/21
Affected Version(s): From (including) 3.15.0 Up to (excluding) 3.18.4					
N/A	05-Dec-2022	9.8	The camel-ldap component allows LDAP Injection when using the	https://camel.apache.org/security/CVE-	A-APA-CAME-191222/22

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			filter option. Users are recommended to either move to the Camel-Spring-Ldap component (which is not affected) or upgrade to 3.14.6 or 3.18.4. **CVE ID : CVE-2022-45046**	2022-45046.html	
Product: manifoldcf					
Affected Version(s): * Up to (including) 2.23					
N/A	07-Dec-2022	5.3	Improper neutralization of special elements used in an LDAP query ('LDAP Injection') vulnerability in ActiveDirectory and Sharepoint ActiveDirectory authority connectors of Apache ManifoldCF allows an attacker to manipulate the LDAP search queries (DoS, additional queries, filter manipulation) during user lookup, if the username or the domain string are passed to the UserACLs servlet without validation. This issue affects Apache ManifoldCF version 2.23 and prior versions. **CVE ID : CVE-2022-45910**	https://lists.apache.org/thread/m693p0dq6jvwwvmy2wnhj6k854z0s444	A-APA-MANI-191222/23
Product: tapestry					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 4.0.0					
Deserialization of Untrusted Data	02-Dec-2022	9.8	** UNSUPPORTED WHEN ASSIGNED ** Apache Tapestry 3.x allows deserialization of	https://lists.apache.org/thread/bwn1vjrvz1hq0wbdzj2	A-APA-TAPE-191222/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			untrusted data, leading to remote code execution. This issue is similar to but distinct from CVE-2020-17531, which applies the the (also unsupported) 4.x version line. NOTE: This vulnerability only affects Apache Tapestry version line 3.x, which is no longer supported by the maintainer. Users are recommended to upgrade to a supported version line of Apache Tapestry. **CVE ID : CVE-2022-46366**	3wz322244swhj	
Vendor: armemberplugin					
Product: armember					
Affected Version(s): * Up to (including) 5.5.1					
Improper Privilege Management	06-Dec-2022	8.8	Unauth. Privilege Escalation vulnerability in ARMember premium plugin <= 5.5.1 on WordPress. **CVE ID : CVE-2022-42888**	N/A	A-ARM-ARME-191222/25
Vendor: Arubanetworks					
Product: airwave					
Affected Version(s): * Up to (including) 8.2.15.0					
N/A	08-Dec-2022	8.1	Vulnerabilities in the AirWave Management Platform web-based management interface exist which expose some URLs to a lack of proper access controls. These vulnerabilities could allow a remote attacker	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-019.txt	A-ARU-AIRW-191222/26

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with limited privileges to gain access to sensitive information and/or change network configurations with privileges at a higher effective level in Aruba AirWave Management Platform version(s): 8.2.15.0 and below. **CVE ID : CVE-2022-37916**		
N/A	08-Dec-2022	8.1	Vulnerabilities in the AirWave Management Platform web-based management interface exist which expose some URLs to a lack of proper access controls. These vulnerabilities could allow a remote attacker with limited privileges to gain access to sensitive information and/or change network configurations with privileges at a higher effective level in Aruba AirWave Management Platform version(s): 8.2.15.0 and below. **CVE ID : CVE-2022-37917**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-019.txt	A-ARU-AIRW-191222/27
N/A	08-Dec-2022	8.1	Vulnerabilities in the AirWave Management Platform web-based management interface exist which expose some URLs to a lack of proper access controls. These vulnerabilities could allow a remote attacker with limited privileges to	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-019.txt	A-ARU-AIRW-191222/28

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gain access to sensitive information and/or change network configurations with privileges at a higher effective level in Aruba AirWave Management Platform version(s): 8.2.15.0 and below. **CVE ID : CVE-2022-37918**		
Product: edgeconnect_enterprise					
Affected Version(s): From (including) 8.3.1.0 Up to (including) 8.3.7.1					
N/A	12-Dec-2022	8.8	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-43542**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/29
N/A	12-Dec-2022	7.5	A vulnerability exists in the API of Aruba EdgeConnect Enterprise. An unauthenticated attacker can exploit this condition via the web-	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/30

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface to create a denial-of-service condition which prevents the appliance from properly responding to API requests in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below; **CVE ID : CVE-2022-37919**		
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37920**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/31
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to	https://www.arubanetworks.com/assets/alert/ARUBA-	A-ARU-EDGE-191222/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37921**	PSA-2022-018.txt	
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37922**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37923**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/34
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below;	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/35

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37924**		
N/A	12-Dec-2022	7.2	A vulnerability in the Aruba EdgeConnect Enterprise web management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-44533**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/36
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Dec-2022	6.5	An authenticated path traversal vulnerability exists in the Aruba EdgeConnect Enterprise command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-44532**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	6.1	A vulnerability within the web-based management interface of Aruba EdgeConnect Enterprise could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37925**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/38
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	5.4	A vulnerability within the web-based management interface of EdgeConnect Enterprise could allow a remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface by uploading a specially crafted file. A successful exploit could	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37926**		
Affected Version(s): From (including) 9.0.0.0 Up to (including) 9.0.7.0					
N/A	12-Dec-2022	8.8	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-43542**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/40
N/A	12-Dec-2022	7.5	A vulnerability exists in the API of Aruba EdgeConnect Enterprise. An unauthenticated	https://www.arubanetworks.com/assets/alert/ARUBA-	A-ARU-EDGE-191222/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can exploit this condition via the web-based management interface to create a denial-of-service condition which prevents the appliance from properly responding to API requests in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below; **CVE ID : CVE-2022-37919**	PSA-2022-018.txt	
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37920**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/42
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line	https://www.arubanetworks.com/assets/	A-ARU-EDGE-191222/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37921**	alert/ARUBA-PSA-2022-018.txt	
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37922**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37923**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/45
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below;	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37924**		
N/A	12-Dec-2022	7.2	A vulnerability in the Aruba EdgeConnect Enterprise web management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-44533**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/47
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Dec-2022	6.5	An authenticated path traversal vulnerability exists in the Aruba EdgeConnect Enterprise command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-44532**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	6.1	A vulnerability within the web-based management interface of Aruba EdgeConnect Enterprise could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37925**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/49
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	5.4	A vulnerability within the web-based management interface of EdgeConnect Enterprise could allow a remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface by uploading a specially crafted file. A successful exploit could	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37926**		
Affected Version(s): From (including) 9.1.0.0 Up to (including) 9.1.3.0					
N/A	12-Dec-2022	8.8	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-43542**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/51
N/A	12-Dec-2022	7.5	A vulnerability exists in the API of Aruba EdgeConnect Enterprise. An unauthenticated	https://www.arubanetworks.com/assets/alert/ARUBA-	A-ARU-EDGE-191222/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can exploit this condition via the web-based management interface to create a denial-of-service condition which prevents the appliance from properly responding to API requests in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below; **CVE ID : CVE-2022-37919**	PSA-2022-018.txt	
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37920**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/53
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line	https://www.arubanetworks.com/assets/	A-ARU-EDGE-191222/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37921**	alert/ARUBA-PSA-2022-018.txt	
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37922**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/55

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37923**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/56
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below;	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37924**		
N/A	12-Dec-2022	7.2	A vulnerability in the Aruba EdgeConnect Enterprise web management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-44533**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/58
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Dec-2022	6.5	An authenticated path traversal vulnerability exists in the Aruba EdgeConnect Enterprise command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-44532**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	6.1	A vulnerability within the web-based management interface of Aruba EdgeConnect Enterprise could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37925**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/60
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	5.4	A vulnerability within the web-based management interface of EdgeConnect Enterprise could allow a remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface by uploading a specially crafted file. A successful exploit could	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/61

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37926**		
Affected Version(s): From (including) 9.2.0.0 Up to (including) 9.2.1.0					
N/A	12-Dec-2022	8.8	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-43542**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/62
N/A	12-Dec-2022	7.5	A vulnerability exists in the API of Aruba EdgeConnect Enterprise. An unauthenticated	https://www.arubanetworks.com/assets/alert/ARUBA-	A-ARU-EDGE-191222/63

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can exploit this condition via the web-based management interface to create a denial-of-service condition which prevents the appliance from properly responding to API requests in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below; **CVE ID : CVE-2022-37919**	PSA-2022-018.txt	
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37920**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/64
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line	https://www.arubanetworks.com/assets/	A-ARU-EDGE-191222/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37921**	alert/ARUBA-PSA-2022-018.txt	
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37922**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37923**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/67
N/A	12-Dec-2022	7.2	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below;	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37924**		
N/A	12-Dec-2022	7.2	A vulnerability in the Aruba EdgeConnect Enterprise web management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-44533**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/69
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Dec-2022	6.5	An authenticated path traversal vulnerability exists in the Aruba EdgeConnect Enterprise command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-44532**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	6.1	A vulnerability within the web-based management interface of Aruba EdgeConnect Enterprise could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37925**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/71
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	5.4	A vulnerability within the web-based management interface of EdgeConnect Enterprise could allow a remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface by uploading a specially crafted file. A successful exploit could	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-018.txt	A-ARU-EDGE-191222/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below. **CVE ID : CVE-2022-37926**		
Product: sd-wan					
Affected Version(s): From (including) 8.7.0.0-2.3.0.0 Up to (excluding) 8.7.0.0-2.3.0.6					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Dec-2022	9.8	There is a command injection vulnerability that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2022-37897**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	A-ARU-SD-W-191222/73
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	8.8	Vulnerabilities in ArubaOS running on 7xxx series controllers exist that allows an attacker to execute arbitrary code during the	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	A-ARU-SD-W-191222/74

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			boot sequence. Successful exploitation could allow an attacker to achieve permanent modification of the underlying operating system. **CVE ID : CVE-2022-37904**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Dec-2022	8.8	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2022-37912**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	A-ARU-SD-W-191222/75
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Dec-2022	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of the vulnerability results in the ability to delete arbitrary files on the underlying operating system. **CVE ID : CVE-2022-37906**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	A-ARU-SD-W-191222/76
N/A	12-Dec-2022	7.5	A vulnerability exists in the ArubaOS bootloader on 7xxx series controllers which can result in a denial of service (DoS) condition on an impacted system. A	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	A-ARU-SD-W-191222/77

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful attacker can cause a system hang which can only be resolved via a power cycle of the impacted controller. **CVE ID : CVE-2022-37907**		
N/A	12-Dec-2022	6.5	An authenticated attacker can impact the integrity of the ArubaOS bootloader on 7xxx series controllers. Successful exploitation can compromise the hardware chain of trust on the impacted controller. **CVE ID : CVE-2022-37908**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	A-ARU-SD-W-191222/78
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Dec-2022	6.5	A buffer overflow vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in a denial of service on the affected system. **CVE ID : CVE-2022-37910**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	A-ARU-SD-W-191222/79
Improper Restriction of XML External Entity Reference	12-Dec-2022	5.5	Due to improper restrictions on XML entities multiple vulnerabilities exist in the command line interface of ArubaOS. A successful exploit could allow an authenticated attacker to retrieve files from the local system or cause the application to consume system	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	A-ARU-SD-W-191222/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resources, resulting in a denial of service condition. **CVE ID : CVE-2022-37911**		
N/A	12-Dec-2022	5.3	Aruba has identified certain configurations of ArubaOS that can lead to sensitive information disclosure from the configured ESSIDs. The scenarios in which disclosure of potentially sensitive information can occur are complex, and depend on factors beyond the control of attackers. **CVE ID : CVE-2022-37909**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	A-ARU-SD-W-191222/81
Vendor: Automattic					
Product: jetpack_crm					
Affected Version(s): * Up to (excluding) 5.4.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	4.8	The Jetpack CRM WordPress plugin before 5.4.3 does not sanitise and escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2022-3919**	N/A	A-AUT-JETP-191222/82
Vendor: automotive_shop_management_system_project					
Product: automotive_shop_management_system					
Affected Version(s): 1.0					
Improper Neutralizat	09-Dec-2022	7.2	Automotive Shop Management System v1.0	N/A	A-AUT-AUTO-191222/83

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			was discovered to contain a SQL injection vulnerability via the id parameter at /services/view_service.php. **CVE ID : CVE-2022-44838**		
Vendor: auto\/taxi_stand_management_system_project					
Product: auto\/taxi_stand_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	AutoTaxi Stand Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component search.php. **CVE ID : CVE-2022-43369**	N/A	A-AUT-AUTO-191222/84
Vendor: Avast					
Product: avast					
Affected Version(s): From (including) 20.5 Up to (including) 22.9					
Improper Privilege Management	06-Dec-2022	8.8	A vulnerability within the malware removal functionality of Avast and AVG Antivirus allowed an attacker with write access to the filesystem, to escalate his privileges in certain scenarios. The issue was fixed with Avast and AVG Antivirus version 22.10. **CVE ID : CVE-2022-4173**	N/A	A-AVA-AVAS-191222/85
Product: avg_antivirus					
Affected Version(s): From (including) 20.5 Up to (including) 22.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	06-Dec-2022	8.8	A vulnerability within the malware removal functionality of Avast and AVG Antivirus allowed an attacker with write access to the filesystem, to escalate his privileges in certain scenarios. The issue was fixed with Avast and AVG Antivirus version 22.10. **CVE ID : CVE-2022-4173**	N/A	A-AVA-AVG_-191222/86
Product: script_shield					
Affected Version(s): * Up to (including) 18.0.1473.0					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Dec-2022	10	The aswjsflt.dll library from Avast Antivirus windows contained a potentially exploitable heap corruption vulnerability that could enable an attacker to bypass the sandbox of the application it was loaded into, if applicable. This issue was fixed in version 18.0.1478 of the Script Shield Component. **CVE ID : CVE-2022-4291**	https://support.norton.com/sp/static/external/tools/security-advisories.html	A-AVA-SCRI-191222/87
Vendor: Awstats					
Product: awstats					
Affected Version(s): From (including) 7.0 Up to (including) 7.8					
Improper Neutralization of Input During Web Page Generation	04-Dec-2022	6.1	AWStats 7.x through 7.8 allows XSS in the hostinfo plugin due to printing a response from Net::XWhois without proper checks.	https://github.com/eldy/AWStats/pull/226	A-AWS-AWST-191222/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2022-46391**		
Vendor: axiell					
Product: iguana					
Affected Version(s): * Up to (including) 4.5.02					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-2022	6.1	A reflected XSS vulnerability has been found in Axiell Iguana CMS, allowing an attacker to execute code in a victim's browser. The title parameter on the twitter.php endpoint does not properly neutralise user input, resulting in the vulnerability. **CVE ID : CVE-2022-45050**	N/A	A-AXI-IGUA-191222/89
Vendor: ayacms_project					
Product: ayacms					
Affected Version(s): 3.1.2					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	07-Dec-2022	9.8	AyaCMS 3.1.2 is vulnerable to Remote Code Execution (RCE). **CVE ID : CVE-2022-45550**	N/A	A-AYA-AYAC-191222/90
Unrestricted Upload of File with Dangerous Type	06-Dec-2022	8.8	AyaCMS v3.1.2 has an Arbitrary File Upload vulnerability. **CVE ID : CVE-2022-45548**	N/A	A-AYA-AYAC-191222/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: background_management_system_project					
Product: background_management_system					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Dec-2022	9.8	A vulnerability was found in Shaoxing Background Management System. It has been declared as critical. This vulnerability affects unknown code of the file /Default/Bd. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-214774 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4277**	N/A	A-BAC-BACK-191222/92
Vendor: Basercms					
Product: basercms					
Affected Version(s): * Up to (excluding) 4.7.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-2022	4.8	Stored cross-site scripting vulnerability in Permission Settings of baserCMS versions prior to 4.7.2 allows a remote authenticated attacker with an administrative privilege to inject an arbitrary script. **CVE ID : CVE-2022-41994**	https://basercms.net/security/JVN_53682526	A-BAS-BASE-191222/93
Improper Neutralization of	07-Dec-2022	4.8	Stored cross-site scripting vulnerability in User group management	https://basercms.net/secur	A-BAS-BASE-191222/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			of baserCMS versions prior to 4.7.2 allows a remote authenticated attacker with an administrative privilege to inject an arbitrary script. **CVE ID : CVE-2022-42486**	ity/JVN_53682526	
Vendor: beappsmobile					
Product: pc_keyboard_wifi\&bluetooth					
Affected Version(s): * Up to (including) 30					
Missing Authentication for Critical Function	05-Dec-2022	9.8	PC Keyboard allows remote unauthenticated users to send instructions to the server to execute arbitrary code without any previous authorization or authentication. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H **CVE ID : CVE-2022-45479**	https://www.synopsys.com/blogs/software-security/cyrc-advisory-remote-code-execution-vulnerabilities-mouse-keyboard-apps/	A-BEA-PC_K-191222/95
Product: pc_keyboard_wifi_\&_bluetooth					
Affected Version(s): * Up to (including) 30					
Cleartext Transmission of Sensitive Information	02-Dec-2022	5.9	PC Keyboard WiFi & Bluetooth allows an attacker (in a man-in-the-middle position between the server and a connected device) to see all data (including keypresses) in cleartext. CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N **CVE ID : CVE-2022-45480**	N/A	A-BEA-PC_K-191222/96
Vendor: beetl-bbs_project					
Product: beetl-bbs					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-2022	5.4	A vulnerability was found in xiandafu beetl-bbs. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file WebUtils.java. The manipulation of the argument user leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-215107. **CVE ID : CVE-2022-4347**	N/A	A-BEE-BEET-191222/97
Vendor: Bluetooth					
Product: bluetooth_core_specification					
Affected Version(s): From (including) 1.1b Up to (including) 5.3					
Authentication Bypass by Capture-replay	12-Dec-2022	7.5	Bluetooth® Pairing in Bluetooth Core Specification v1.0B through v5.3 may permit an unauthenticated MITM to acquire credentials with two pairing devices via adjacent access when at least one device supports BR/EDR Secure Connections pairing and the other BR/EDR Legacy PIN code pairing if the MITM negotiates BR/EDR Secure Simple Pairing in Secure Connections mode using the Passkey association	https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/reporting-security/	A-BLU-BLUE-191222/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			model with the pairing Initiator and BR/EDR Legacy PIN code pairing with the pairing Responder and brute forces the Passkey entered by the user into the Responder as a 6-digit PIN code. The MITM attacker can use the identified PIN code value as the Passkey value to complete authentication with the Initiator via Bluetooth pairing method confusion. **CVE ID : CVE-2022-25837**		
Affected Version(s): From (including) 4.0 Up to (including) 5.3					
Authentication Bypass by Capture-replay	12-Dec-2022	7.5	Bluetooth® Low Energy Pairing in Bluetooth Core Specification v4.0 through v5.3 may permit an unauthenticated MITM to acquire credentials with two pairing devices via adjacent access when the MITM negotiates Legacy Passkey Pairing with the pairing Initiator and Secure Connections Passkey Pairing with the pairing Responder and brute forces the Passkey entered by the user into the Initiator. The MITM attacker can use the identified Passkey value to complete authentication with the Responder via Bluetooth	https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/reporting-security/	A-BLU-BLUE-191222/99

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pairing method confusion. **CVE ID : CVE-2022-25836**		
Vendor: book_store_management_system_project					
Product: book_store_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	5.4	A cross-site scripting (XSS) vulnerability in Book Store Management System v1.0.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter under the Add New System User module. **CVE ID : CVE-2022-45215**	N/A	A-BOO-BOOK-191222/100
Affected Version(s): 1.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-2022	5.4	A cross-site scripting (XSS) vulnerability in Book Store Management System v1.0.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Level parameter under the Add New System User module. **CVE ID : CVE-2022-45217**	N/A	A-BOO-BOOK-191222/101
Vendor: boxystudio					
Product: cooked					
Affected Version(s): * Up to (excluding) 1.7.5.7					
Deserialization of	12-Dec-2022	9.8	The Cooked Pro WordPress plugin before	N/A	A-BOX-COOK-191222/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Data			1.7.5.7 does not properly validate or sanitize the recipe_args parameter before unserializing it in the cooked_loadmore action, allowing an unauthenticated attacker to trigger a PHP Object injection vulnerability. **CVE ID : CVE-2022-3900**		
Vendor: Broadcom					
Product: brocade_sannav					
Affected Version(s): * Up to (excluding) 2.2.1					
Insertion of Sensitive Information into Log File	09-Dec-2022	4.9	Brocade SANnav before v2.2.1 logs usernames and encoded passwords in debug-enabled logs. The vulnerability could allow an attacker with admin privilege to read sensitive information. **CVE ID : CVE-2022-33187**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2122	A-BRO-BROC-191222/103
Product: symantec_endpoint_protection					
Affected Version(s): * Up to (excluding) 14.3.5.1					
Incorrect Authorization	01-Dec-2022	7.5	Symantec Endpoint Protection (Windows) agent, prior to 14.3 RU6/14.3 RU5 Patch 1, may be susceptible to a Security Control Bypass vulnerability, which is a type of issue that can potentially allow a threat actor to circumvent existing security controls. This CVE applies narrowly to the Client User Interface	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/21014	A-BRO-SYMA-191222/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Password protection and Policy Import/Export Password protection, if it has been enabled. **CVE ID : CVE-2022-37017**		
Affected Version(s): * Up to (including) 14.3.5					
Improper Privilege Management	01-Dec-2022	9.8	Symantec Endpoint Protection (Windows) agent may be susceptible to a Privilege Escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user. **CVE ID : CVE-2022-37016**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/21014	A-BRO-SYMA-191222/105
Vendor: BT					
Product: baota					
Affected Version(s): From (including) 7.9.4 Up to (including) 7.9.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-2022	5.4	In BAOTA linux panel there exists a stored xss vulnerability attackers can use to obtain sensitive information via the log analysis feature. **CVE ID : CVE-2022-4336**	N/A	A-BT-BAOT-191222/106
Vendor: buddybadges_project					
Product: buddybadges					
Affected Version(s): * Up to (including) 1.0.0					
Improper Neutralization of	12-Dec-2022	7.2	The buddybadges WordPress plugin through 1.0.0 does not	N/A	A-BUD-BUDD-191222/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users **CVE ID : CVE-2022-3925**		
Vendor: Cacti					
Product: cacti					
Affected Version(s): * Up to (including) 1.2.22					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Dec-2022	9.8	Cacti is an open source platform which provides a robust and extensible operational monitoring and fault management framework for users. In affected versions a command injection vulnerability allows an unauthenticated user to execute arbitrary code on a server running Cacti, if a specific data source was selected for any monitored device. The vulnerability resides in the `remote_agent.php` file. This file can be accessed without authentication. This function retrieves the IP address of the client via `get_client_addr` and resolves this IP address to the corresponding hostname via `gethostbyaddr`. After this, it is verified that an entry within the `poller` table exists, where the	https://github.com/Cacti/cacti/security/advisories/GHSA-6p93-p743-35gf, https://github.com/Cacti/cacti/commit/b43f13ae7f1e6bfe4e8e56a80a7cd867cf2db52b, https://github.com/Cacti/cacti/commit/a8d59e8fa5f0054aa9c6981b1cbe30ef0e2a0ec9	A-CAC-CACT-191222/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hostname corresponds to the resolved hostname. If such an entry was found, the function returns `true` and the client is authorized. This authorization can be bypassed due to the implementation of the `get_client_addr` function. The function is defined in the file `lib/functions.php` and checks serval `$_SERVER` variables to determine the IP address of the client. The variables beginning with `HTTP_` can be arbitrarily set by an attacker. Since there is a default entry in the `poller` table with the hostname of the server running Cacti, an attacker can bypass the authentication e.g. by providing the header `Forwarded-For: <TARGETIP>`. This way the function `get_client_addr` returns the IP address of the server running Cacti. The following call to `gethostbyaddr` will resolve this IP address to the hostname of the server, which will pass the `poller` hostname check because of the default entry. After the authorization of the `remote_agent.php` file is bypassed, an attacker		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can trigger different actions. One of these actions is called `polldata`. The called function `poll_for_data` retrieves a few request parameters and loads the corresponding `poller_item` entries from the database. If the `action` of a `poller_item` equals `POLLER_ACTION_SCRIPT_PHP`, the function `proc_open` is used to execute a PHP script. The attacker-controlled parameter `$poller_id` is retrieved via the function `get_nfilter_request_var`, which allows arbitrary strings. This variable is later inserted into the string passed to `proc_open`, which leads to a command injection vulnerability. By e.g. providing the `poller_id=;id` the `id` command is executed. In order to reach the vulnerable call, the attacker must provide a `host_id` and `local_data_id`, where the `action` of the corresponding `poller_item` is set to `POLLER_ACTION_SCRIPT_PHP`. Both of these ids (`host_id` and `local_data_id`) can easily be bruteforced. The only requirement is that a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`poller_item` with an `POLLER_ACTION_SCRIPT_PHP` action exists. This is very likely on a productive instance because this action is added by some predefined templates like `Device - Uptime` or `Device - Polling Time`. This command injection vulnerability allows an unauthenticated user to execute arbitrary commands if a `poller_item` with the `action` type `POLLER_ACTION_SCRIPT_PHP` (`2`) is configured. The authorization bypass should be prevented by not allowing an attacker to make `get_client_addr` (file `lib/functions.php`) return an arbitrary IP address. This could be done by not honoring the `HTTP_...` `$_SERVER` variables. If these should be kept for compatibility reasons it should at least be prevented to fake the IP address of the server running Cacti. This vulnerability has been addressed in both the 1.2.x and 1.3.x release branches with `1.2.23` being the first release containing the patch. **CVE ID : CVE-2022-46169**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Call-cc					
Product: chicken					
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.3.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-Dec-2022	9.8	egg-compile.scm in CHICKEN 5.x before 5.3.1 allows arbitrary OS command execution during package installation via escape characters in a .egg file. **CVE ID : CVE-2022-45145**	https://lists.gnu.org/archive/html/chicken-announce/2022-11/msg00000.html	A-CAL-CHIC-191222/109
Vendor: Canon					
Product: vitrea_view					
Affected Version(s): * Up to (excluding) 7.8					
Authorization Bypass Through User-Controlled Key	09-Dec-2022	6.5	Canon Medical Informatics Vitrea Vision 7.7.76.1 does not adequately enforce access controls. An authenticated user is able to gain unauthorized access to imaging records by tampering with the vitrea-view/studies/search patientId parameter. **CVE ID : CVE-2022-38765**	https://www.vitalimages.com/customer-success-support-program/vital-images-software-security-updates/	A-CAN-VITR-191222/110
Vendor: canteen_management_system_project					
Product: canteen_management_system					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an	11-Dec-2022	8.8	A vulnerability classified as critical was found in SourceCodester Canteen Management System. This vulnerability affects unknown code of the file	N/A	A-CAN-CANT-191222/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			ajax_represent.php. The manipulation of the argument customer_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-215272. **CVE ID : CVE-2022-4403**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-2022	6.1	A vulnerability was found in SourceCodester Canteen Management System. It has been classified as problematic. This affects the function builtin_echo of the file categories.php. 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. The identifier VDB-214629 was assigned to this vulnerability. **CVE ID : CVE-2022-4252**	N/A	A-CAN-CANT-191222/112
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-2022	5.4	A vulnerability was found in SourceCodester Canteen Management System. It has been declared as problematic. This vulnerability affects the function builtin_echo of the file customer.php. The manipulation leads to cross site scripting.	N/A	A-CAN-CANT-191222/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-214630 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4253**		
Vendor: casbin					
Product: casdoor					
Affected Version(s): * Up to (excluding) 1.126.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Dec-2022	8.1	Casdoor before v1.126.1 was discovered to contain an arbitrary file deletion vulnerability via the uploadFile function. **CVE ID : CVE-2022-44942**	https://github.com/casdoor/casdoor/issues/1171	A-CAS-CASD-191222/114
Vendor: cdatatec					
Product: c-data_web_management_system					
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-Dec-2022	9.8	A vulnerability was found in C-DATA Web Management System. It has been rated as critical. This issue affects some unknown processing of the file cgi-bin/jumpto.php of the component GET Parameter Handler. The manipulation of the argument hostname leads to argument injection. The attack may be initiated remotely. The exploit has been	N/A	A-CDA-C-DA-191222/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-214631. **CVE ID : CVE-2022-4257**		
Vendor: certifi_project					
Product: certifi					
Affected Version(s): 2022.12.07					
Insufficient Verification of Data Authenticity	07-Dec-2022	7.5	Certifi is a curated collection of Root Certificates for validating the trustworthiness of SSL certificates while verifying the identity of TLS hosts. Certifi 2022.12.07 removes root certificates from "TrustCor" from the root store. These are in the process of being removed from Mozilla's trust store. TrustCor's root certificates are being removed pursuant to an investigation prompted by media reporting that TrustCor's ownership also operated a business that produced spyware. Conclusions of Mozilla's investigation can be found in the linked google group discussion. **CVE ID : CVE-2022-23491**	N/A	A-CER-CERT-191222/116
Vendor: clastix					
Product: capsule					
Affected Version(s): * Up to (excluding) 0.1.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	02-Dec-2022	8.8	Capsule is a multi-tenancy and policy-based framework for Kubernetes. Prior to version 0.1.3, a ServiceAccount deployed in a Tenant Namespace, when granted with `PATCH` capabilities on its own Namespace, is able to edit it and remove the Owner Reference, breaking the reconciliation of the Capsule Operator and removing all the enforcement like Pod Security annotations, Network Policies, Limit Range and Resource Quota items. An attacker could detach the Namespace from a Tenant that is forbidding starting privileged Pods using the Pod Security labels by removing the OwnerReference, removing the enforcement labels, and being able to start privileged containers that would be able to start a generic Kubernetes privilege escalation. Patches have been released for version 0.1.3. No known workarounds are available. **CVE ID : CVE-2022-46167**	https://github.com/clastix/capsule/commit/1df430e71be8c4778c82eca3459978ad7d0b4b7b, https://github.com/clastix/capsule/commit/75525ac19254b0c5111e34d7985e2be7bc8b1ac1, https://github.com/clastix/capsule/releases/tag/v0.1.3	A-CLA-CAPS-191222/117
Vendor: clerk					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: clerk.io					
Affected Version(s): * Up to (excluding) 4.0.0					
Exposure of Sensitive Information to an Unauthorized Actor	05-Dec-2022	7.5	The Clerk WordPress plugin before 4.0.0 is affected by time-based attacks in the validation function for all API requests due to the usage of comparison operators to verify API keys against the ones stored in the site options. **CVE ID : CVE-2022-3907**	N/A	A-CLE-CLER-191222/118
Vendor: clicshopping					
Product: clicshopping_v3					
Affected Version(s): 3.402					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in ClicShopping_V3 v3.402 allows attackers to execute arbitrary web scripts or HTML via a crafted URL parameter. **CVE ID : CVE-2022-45769**	N/A	A-CLI-CLIC-191222/119
Vendor: codecentric					
Product: spring_boot_admin					
Affected Version(s): * Up to (excluding) 2.6.10					
Improper Control of Generation of Code ('Code Injection')	09-Dec-2022	9.8	Spring boot admins is an open source administrative user interface for management of spring boot applications. All users who run Spring Boot Admin Server, having enabled Notifiers (e.g. Teams-Notifier) and write access to	https://github.com/codecentric/spring-boot-admin/commit/c14c3ec12533f71f84de9ce3ce5ceb7991975f75	A-COD-SPRI-191222/120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			environment variables via UI are affected. Users are advised to upgrade to the most recent releases of Spring Boot Admin 2.6.10 and 2.7.8 to resolve this issue. Users unable to upgrade may disable any notifier or disable write access (POST request) on `/env` actuator endpoint. **CVE ID : CVE-2022-46166**		
Affected Version(s): 3.0.0					
Improper Control of Generation of Code ('Code Injection')	09-Dec-2022	9.8	Spring boot admins is an open source administrative user interface for management of spring boot applications. All users who run Spring Boot Admin Server, having enabled Notifiers (e.g. Teams-Notifier) and write access to environment variables via UI are affected. Users are advised to upgrade to the most recent releases of Spring Boot Admin 2.6.10 and 2.7.8 to resolve this issue. Users unable to upgrade may disable any notifier or disable write access (POST request) on `/env` actuator endpoint. **CVE ID : CVE-2022-46166**	https://github.com/codecentric/spring-boot-admin/commit/c14c3ec12533f71f84de9ce3ce5ceb7991975f75	A-COD-SPRI-191222/121
Affected Version(s): From (including) 2.7.0 Up to (excluding) 2.7.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	09-Dec-2022	9.8	Spring boot admins is an open source administrative user interface for management of spring boot applications. All users who run Spring Boot Admin Server, having enabled Notifiers (e.g. Teams-Notifier) and write access to environment variables via UI are affected. Users are advised to upgrade to the most recent releases of Spring Boot Admin 2.6.10 and 2.7.8 to resolve this issue. Users unable to upgrade may disable any notifier or disable write access (POST request) on `/env` actuator endpoint. **CVE ID : CVE-2022-46166**	https://github.com/codecentric/spring-boot-admin/commit/c14c3ec12533f71f84de9ce3ce5ceb7991975f75	A-COD-SPRI-191222/122
Vendor: coder-chain_gdut_project					
Product: coder-chain_gdut					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-2022	6.1	A vulnerability has been found in csliuwy coder-chain_gdut and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /back/index.php/user/User/?1. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public	N/A	A-COD-CODE-191222/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and may be used. The associated identifier of this vulnerability is VDB-215095. **CVE ID : CVE-2022-4341**		
Vendor: collne					
Product: welcart_e-commerce					
Affected Version(s): * Up to (excluding) 2.8.4					
Cross-Site Request Forgery (CSRF)	12-Dec-2022	6.5	The Welcart e-Commerce WordPress plugin before 2.8.4 does not have authorisation and CSRF in an AJAX action, allowing any logged-in user to create, update and delete shipping methods. **CVE ID : CVE-2022-3946**	N/A	A-COL-WELC-191222/124
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	5.4	The Welcart e-Commerce WordPress plugin before 2.8.4 does not sanitise and escape some parameters, which could allow any authenticated users, such as subscriber to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2022-3935**	N/A	A-COL-WELC-191222/125
Vendor: concretecms					
Product: concrete_cms					
Affected Version(s): * Up to (excluding) 8.5.10					
Improper Neutralization of Input During Web Page	05-Dec-2022	6.1	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to XSS in the text input field since the result	https://documentation.concretecms.org/developers/introduction/version-	A-CON-CONC-191222/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			dashboard page output is not sanitized. The Concrete CMS security team has ranked this 4.2 with CVSS v3.1 vector AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N Thanks @_akbar_jafarli_ for reporting. Remediate by updating to Concrete CMS 8.5.10 and Concrete CMS 9.1.3. **CVE ID : CVE-2022-43556**	history/8510-release-notes, https://documentation.concretecms.org/developers/introduction/version-history/913-release-notes	
Affected Version(s): 9.1.3					
XML Injection (aka Blind XPath Injection)	05-Dec-2022	7.5	ConcreteCMS v9.1.3 was discovered to be vulnerable to Xpath injection attacks. This vulnerability allows attackers to access sensitive XML data via a crafted payload injected into the URL path folder "3". **CVE ID : CVE-2022-46464**	N/A	A-CON-CONC-191222/127
Affected Version(s): From (including) 9.0.0 Up to (including) 9.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	6.1	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to XSS in the text input field since the result dashboard page output is not sanitized. The Concrete CMS security team has ranked this 4.2 with CVSS v3.1 vector AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N Thanks @_akbar_jafarli_ for	https://documentation.concretecms.org/developers/introduction/version-history/8510-release-notes, https://documentation.concretecms.org/developers/introduction/version-	A-CON-CONC-191222/128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reporting. Remediate by updating to Concrete CMS 8.5.10 and Concrete CMS 9.1.3. **CVE ID : CVE-2022-43556**	history/913-release-notes	
Vendor: contest-gallery					
Product: contest_gallery					
Affected Version(s): * Up to (including) 13.1.0.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Contest Gallery plugin <= 13.1.0.9 on WordPress. **CVE ID : CVE-2022-45848**	N/A	A-CON-CONT-191222/129
Vendor: Craftcms					
Product: craft_cms					
Affected Version(s): From (including) 3.0.0 Up to (including) 3.7.32					
Missing Encryption of Sensitive Data	05-Dec-2022	7.5	All Craft CMS versions between 3.0.0 and 3.7.32 disclose password hashes of users who authenticate using their E-Mail address or username in Anti-CSRF-Tokens. Craft CMS uses a cookie called CRAFT_CSRF_TOKEN and a HTML hidden field called CRAFT_CSRF_TOKEN to avoid Cross Site Request Forgery attacks. The CRAFT_CSRF_TOKEN cookie discloses the password hash in without encoding it whereas the	N/A	A-CRA-CRAF-191222/130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			corresponding HTML hidden field discloses the users' password hash in a masked manner, which can be decoded by using public functions of the YII framework. **CVE ID : CVE-2022-37783**		
Vendor: crowdstrike					
Product: falcon					
Affected Version(s): 6.44.15806					
Incorrect Authorization	04-Dec-2022	4.9	CrowdStrike Falcon 6.44.15806 allows an administrative attacker to uninstall Falcon Sensor, bypassing the intended protection mechanism in which uninstallation requires possessing a one-time token. (The sensor is managed at the kernel level.) **CVE ID : CVE-2022-44721**	N/A	A-CRO-FALC-191222/131
Vendor: cube					
Product: cube.js					
Affected Version(s): 0.31.23					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Dec-2022	8.8	cube-js is a headless business intelligence platform. In version 0.31.23 all authenticated Cube clients could bypass SQL row-level security and run arbitrary SQL via the newly introduced /v1/sql-runner endpoint. This issue has been resolved in version	https://github.com/cube-js/cube.js/commit/3c614674fed6ca17df08bbba8c835ef110167570, https://github.com/cube-js/cube.js/commit/f1140de508e359970	A-CUB-CUBE-191222/132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0.31.24. Users are advised to either upgrade to 0.31.24 or to downgrade to 0.31.22. There are no known workarounds for this vulnerability. **CVE ID : CVE-2022-23510**	ac82b50bae1c4bf152f6041	
Vendor: Cybozu					
Product: cybozu_remote_service					
Affected Version(s): From (including) 4.0.0 Up to (including) 4.0.3					
Uncontrolled Resource Consumption	07-Dec-2022	7.5	Uncontrolled resource consumption vulnerability in Cybozu Remote Service 4.0.0 to 4.0.3 allows a remote authenticated attacker to consume huge storage space, which may result in a denial-of-service (DoS) condition. **CVE ID : CVE-2022-44608**	https://cs.cybozu.co.jp/2022/007754.html	A-CYB-CYBO-191222/133
Vendor: daloradius					
Product: daloradius					
Affected Version(s): -					
Exposure of Resource to Wrong Sphere	08-Dec-2022	7.5	Exposure of Sensitive System Information to an Unauthorized Control Sphere in GitHub repository lirantal/daloradius prior to master branch. **CVE ID : CVE-2022-4366**	https://huntr.dev/bounties/f225d69a-d971-410d-a8f9-b0026143aed8, https://github.com/lirantal/daloradius/commit/3d11f375a76ddb3741200296e15	A-DAL-DALO-191222/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				f81d82dfb80ce	
Affected Version(s): * Up to (excluding) 1.3					
Cross-Site Request Forgery (CSRF)	06-Dec-2022	8.8	daloRADIUS is an open source RADIUS web management application. daloRadius 1.3 and prior are vulnerable to a combination cross site scripting (XSS) and cross site request forgery (CSRF) vulnerability which leads to account takeover in the mng-del.php file because of an unescaped variable reflected in the DOM on line 116. This issue has been addressed in commit `ec3b4a419e`. Users are advised to manually apply the commit in order to mitigate this issue. Users may also mitigate this issue with in two parts 1) The CSRF vulnerability can be mitigated by making the daloRadius session cookie to samesite=Lax or by the implimentation of a CSRF token in all forms. 2) The XSS vulnerability may be mitigated by escaping it or by introducing a Content-Security policy. **CVE ID : CVE-2022-23475**	https://github.com/lirantal/daloradius/commit/ec3b4a419e20540cf28ce60e48998b893e3f1dea	A-DAL-DALO-191222/135
Vendor: deltaww					
Product: dialink					
Affected Version(s): * Up to (excluding) 1.5.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Dec-2022	7.5	Delta Industrial Automation DIALink versions prior to v1.5.0.0 Beta 4 uses an external input to construct a pathname intended to identify a file or directory located underneath a restricted parent directory. However, the software does not properly neutralize special elements within the pathname, which can cause the pathname to resolve to a location outside of the restricted directory. **CVE ID : CVE-2022-2969**	N/A	A-DEL-DIAL-191222/136
Affected Version(s): 1.5.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Dec-2022	7.5	Delta Industrial Automation DIALink versions prior to v1.5.0.0 Beta 4 uses an external input to construct a pathname intended to identify a file or directory located underneath a restricted parent directory. However, the software does not properly neutralize special elements within the pathname, which can cause the pathname to resolve to a location outside of the restricted directory.	N/A	A-DEL-DIAL-191222/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2969		
Vendor: Dev4press					
Product: gd_bbpress_attachments					
Affected Version(s): * Up to (including) 4.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	5.4	Auth. Stored Cross-Site Scripting (XSS) vulnerability in GD bbPress Attachments plugin <= 4.3.1 on WordPress. **CVE ID : CVE-2022-45816**	N/A	A-DEV-GD_B-191222/138
Vendor: devolutions					
Product: remote_desktop_manager					
Affected Version(s): From (including) 2022.3.13 Up to (excluding) 2022.3.26					
N/A	12-Dec-2022	8.8	Elevation of privilege in the Azure SQL Data Source in Devolutions Remote Desktop Manager 2022.3.13 to 2022.3.24 allows an authenticated user to spoof a privileged account. **CVE ID : CVE-2022-3641**	N/A	A-DEV-REMO-191222/139
Vendor: dhis2					
Product: dhis_2					
Affected Version(s): 2.39.0					
Improper Privilege Management	08-Dec-2022	7.2	DHIS 2 is an open source information system for data capture, management, validation, analytics and visualization. Affected versions are subject to a privilege escalation	N/A	A-DHI-DHIS-191222/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. A DHIS2 user with authority to manage users can assign superuser privileges to themself by manually crafting an HTTP PUT request. Only users with the following DHIS2 user role authorities can exploit this vulnerability. Note that in many systems the only users with user admin privileges are also superusers. In these cases, the escalation vulnerability does not exist. The vulnerability is only exploitable by attackers who can authenticate as users with the user admin authority. As this is usually a small and relatively trusted set of users, exploit vectors will often be limited. DHIS2 administrators should upgrade to the following hotfix releases: 2.36.12.1, 2.37.8.1, 2.38.2.1, 2.39.0.1. The only known workaround to this issue is to avoid the assignment of the user management authority to any users until the patch has been applied. **CVE ID : CVE-2022-41948**		
Improper Neutralization of	08-Dec-2022	5.4	DHIS 2 is an open source information system for data capture,	N/A	A-DHI-DHIS-191222/141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			management, validation, analytics and visualization. Through various features of DHIS2, an authenticated user may be able to upload a file which includes embedded javascript. The user could then potentially trick another authenticated user to open the malicious file in a browser which would trigger the javascript code, resulting in a cross-site scripting (XSS) attack. DHIS2 administrators should upgrade to the following hotfix releases: 2.36.12.1, 2.37.8.1, 2.38.2.1, 2.39.0.1. Users unable to upgrade may add the following simple CSP rule in your web proxy to the vulnerable endpoints: `script-src 'none'`. This workaround will prevent all javascript from running on those endpoints. **CVE ID : CVE-2022-41947**		
Server-Side Request Forgery (SSRF)	08-Dec-2022	4.3	DHIS 2 is an open source information system for data capture, management, validation, analytics and visualization. In affected versions an authenticated DHIS2 user can craft a request	https://github.com/dhis2/dhis2-core/commit/dc3166c216da53e12a16bfdc51055823b838c1c3	A-DHI-DHIS-191222/142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to DHIS2 to instruct the server to make requests to external resources (like third party servers). This could allow an attacker, for example, to identify vulnerable services which might not be otherwise exposed to the public internet or to determine whether a specific file is present on the DHIS2 server. DHIS2 administrators should upgrade to the following hotfix releases: 2.36.12.1, 2.37.8.1, 2.38.2.1, 2.39.0.1. At this time, there is no known workaround or mitigation for this vulnerability. **CVE ID : CVE-2022-41949**		
Affected Version(s): From (including) 2.34.0 Up to (excluding) 2.36.12.1					
Improper Privilege Management	08-Dec-2022	7.2	DHIS 2 is an open source information system for data capture, management, validation, analytics and visualization. Affected versions are subject to a privilege escalation vulnerability. A DHIS2 user with authority to manage users can assign superuser privileges to themself by manually crafting an HTTP PUT request. Only users with the following DHIS2 user role authorities can exploit this vulnerability.	N/A	A-DHI-DHIS-191222/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note that in many systems the only users with user admin privileges are also superusers. In these cases, the escalation vulnerability does not exist. The vulnerability is only exploitable by attackers who can authenticate as users with the user admin authority. As this is usually a small and relatively trusted set of users, exploit vectors will often be limited. DHIS2 administrators should upgrade to the following hotfix releases: 2.36.12.1, 2.37.8.1, 2.38.2.1, 2.39.0.1. The only known workaround to this issue is to avoid the assignment of the user management authority to any users until the patch has been applied. **CVE ID : CVE-2022-41948**		
Server-Side Request Forgery (SSRF)	08-Dec-2022	4.3	DHIS 2 is an open source information system for data capture, management, validation, analytics and visualization. In affected versions an authenticated DHIS2 user can craft a request to DHIS2 to instruct the server to make requests to external resources (like third party servers).	https://github.com/dhis2/dhis2-core/commit/dc3166c216da53e12a16bfdc51055823b838c1c3	A-DHI-DHIS-191222/144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could allow an attacker, for example, to identify vulnerable services which might not be otherwise exposed to the public internet or to determine whether a specific file is present on the DHIS2 server. DHIS2 administrators should upgrade to the following hotfix releases: 2.36.12.1, 2.37.8.1, 2.38.2.1, 2.39.0.1. At this time, there is no known workaround or mitigation for this vulnerability. **CVE ID : CVE-2022-41949**		
Affected Version(s): From (including) 2.35.0 Up to (excluding) 2.36.12.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-2022	5.4	DHIS 2 is an open source information system for data capture, management, validation, analytics and visualization. Through various features of DHIS2, an authenticated user may be able to upload a file which includes embedded javascript. The user could then potentially trick another authenticated user to open the malicious file in a browser which would trigger the javascript code, resulting in a cross-site scripting (XSS) attack. DHIS2 administrators should	N/A	A-DHI-DHIS-191222/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade to the following hotfix releases: 2.36.12.1, 2.37.8.1, 2.38.2.1, 2.39.0.1. Users unable to upgrade may add the following simple CSP rule in your web proxy to the vulnerable endpoints: `script-src 'none'`. This workaround will prevent all javascript from running on those endpoints. **CVE ID : CVE-2022-41947**		
Affected Version(s): From (including) 2.37.0 Up to (excluding) 2.37.8.1					
Improper Privilege Management	08-Dec-2022	7.2	DHIS 2 is an open source information system for data capture, management, validation, analytics and visualization. Affected versions are subject to a privilege escalation vulnerability. A DHIS2 user with authority to manage users can assign superuser privileges to themself by manually crafting an HTTP PUT request. Only users with the following DHIS2 user role authorities can exploit this vulnerability. Note that in many systems the only users with user admin privileges are also superusers. In these cases, the escalation vulnerability does not exist. The vulnerability is only exploitable by	N/A	A-DHI-DHIS-191222/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers who can authenticate as users with the user admin authority. As this is usually a small and relatively trusted set of users, exploit vectors will often be limited. DHIS2 administrators should upgrade to the following hotfix releases: 2.36.12.1, 2.37.8.1, 2.38.2.1, 2.39.0.1. The only known workaround to this issue is to avoid the assignment of the user management authority to any users until the patch has been applied. **CVE ID : CVE-2022-41948**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-2022	5.4	DHIS 2 is an open source information system for data capture, management, validation, analytics and visualization. Through various features of DHIS2, an authenticated user may be able to upload a file which includes embedded javascript. The user could then potentially trick another authenticated user to open the malicious file in a browser which would trigger the javascript code, resulting in a cross-site scripting (XSS) attack. DHIS2 administrators should	N/A	A-DHI-DHIS-191222/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade to the following hotfix releases: 2.36.12.1, 2.37.8.1, 2.38.2.1, 2.39.0.1. Users unable to upgrade may add the following simple CSP rule in your web proxy to the vulnerable endpoints: `script-src 'none'`. This workaround will prevent all javascript from running on those endpoints. **CVE ID : CVE-2022-41947**		
Server-Side Request Forgery (SSRF)	08-Dec-2022	4.3	DHIS 2 is an open source information system for data capture, management, validation, analytics and visualization. In affected versions an authenticated DHIS2 user can craft a request to DHIS2 to instruct the server to make requests to external resources (like third party servers). This could allow an attacker, for example, to identify vulnerable services which might not be otherwise exposed to the public internet or to determine whether a specific file is present on the DHIS2 server. DHIS2 administrators should upgrade to the following hotfix releases: 2.36.12.1, 2.37.8.1, 2.38.2.1, 2.39.0.1. At this time, there is no known	https://github.com/dhis2/dhis2-core/commit/dc3166c216da53e12a16bfdc51055823b838c1c3	A-DHI-DHIS-191222/148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workaround or mitigation for this vulnerability. **CVE ID : CVE-2022-41949**		
Affected Version(s): From (including) 2.38.0 Up to (excluding) 2.38.2.1					
Improper Privilege Management	08-Dec-2022	7.2	DHIS 2 is an open source information system for data capture, management, validation, analytics and visualization. Affected versions are subject to a privilege escalation vulnerability. A DHIS2 user with authority to manage users can assign superuser privileges to themself by manually crafting an HTTP PUT request. Only users with the following DHIS2 user role authorities can exploit this vulnerability. Note that in many systems the only users with user admin privileges are also superusers. In these cases, the escalation vulnerability does not exist. The vulnerability is only exploitable by attackers who can authenticate as users with the user admin authority. As this is usually a small and relatively trusted set of users, exploit vectors will often be limited. DHIS2 administrators should upgrade to the following	N/A	A-DHI-DHIS-191222/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hotfix releases: 2.36.12.1, 2.37.8.1, 2.38.2.1, 2.39.0.1. The only known workaround to this issue is to avoid the assignment of the user management authority to any users until the patch has been applied. **CVE ID : CVE-2022-41948**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-2022	5.4	DHIS 2 is an open source information system for data capture, management, validation, analytics and visualization. Through various features of DHIS2, an authenticated user may be able to upload a file which includes embedded javascript. The user could then potentially trick another authenticated user to open the malicious file in a browser which would trigger the javascript code, resulting in a cross-site scripting (XSS) attack. DHIS2 administrators should upgrade to the following hotfix releases: 2.36.12.1, 2.37.8.1, 2.38.2.1, 2.39.0.1. Users unable to upgrade may add the following simple CSP rule in your web proxy to the vulnerable endpoints: `script-src 'none'`. This workaround will prevent	N/A	A-DHI-DHIS-191222/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all javascript from running on those endpoints. **CVE ID : CVE-2022-41947**		
Server-Side Request Forgery (SSRF)	08-Dec-2022	4.3	DHIS 2 is an open source information system for data capture, management, validation, analytics and visualization. In affected versions an authenticated DHIS2 user can craft a request to DHIS2 to instruct the server to make requests to external resources (like third party servers). This could allow an attacker, for example, to identify vulnerable services which might not be otherwise exposed to the public internet or to determine whether a specific file is present on the DHIS2 server. DHIS2 administrators should upgrade to the following hotfix releases: 2.36.12.1, 2.37.8.1, 2.38.2.1, 2.39.0.1. At this time, there is no known workaround or mitigation for this vulnerability. **CVE ID : CVE-2022-41949**	https://github.com/dhis2/dhis2-core/commit/dc3166c216da53e12a16bfdc51055823b838c1c3	A-DHI-DHIS-191222/151
Vendor: discourse					
Product: discourse					
Affected Version(s): * Up to (including) 2.8.13					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	02-Dec-2022	4.3	Discourse is an open-source discussion platform. In version 2.8.13 and prior on the `stable` branch and version 2.9.0.beta14 and prior on the `beta` and `tests-passed` branches, any authenticated user can create an unlisted topic. These topics, which are not readily available to other users, can take up unnecessary site resources. A patch for this issue is available in the `main` branch of Discourse. There are no known workarounds available. **CVE ID : CVE-2022-46159**	https://github.com/discourse/discourse/commit/0ce38bd7bce862db251b882613ab7053ca777382	A-DIS-DISC-191222/152
Affected Version(s): 2.9.0					
Allocation of Resources Without Limits or Throttling	02-Dec-2022	4.3	Discourse is an open-source discussion platform. In version 2.8.13 and prior on the `stable` branch and version 2.9.0.beta14 and prior on the `beta` and `tests-passed` branches, any authenticated user can create an unlisted topic. These topics, which are not readily available to other users, can take up unnecessary site resources. A patch for this issue is available in the `main` branch of Discourse. There are no known workarounds available.	https://github.com/discourse/discourse/commit/0ce38bd7bce862db251b882613ab7053ca777382	A-DIS-DISC-191222/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46159		
Vendor: docsys_project					
Product: docsys					
Affected Version(s): * Up to (including) 2.02.37					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	11-Dec-2022	7.2	A vulnerability classified as critical has been found in RainyGao DocSys 2.02.37. This affects an unknown part of the component ZIP File Decompression Handler. The manipulation leads to path traversal: '../filedir'. 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-215271. **CVE ID : CVE-2022-4402**	N/A	A-DOC-DOCS-191222/154
Vendor: dottech					
Product: smart_campus_system					
Affected Version(s): -					
N/A	03-Dec-2022	7.5	A vulnerability, which was classified as problematic, has been found in Dot Tech Smart Campus System. Affected by this issue is some unknown functionality of the file /services/Card/findUser. The manipulation leads to information disclosure. The attack may be launched remotely. The exploit has	N/A	A-DOT-SMAR-191222/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. VDB-214778 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4280**		
Vendor: dpdgroup					
Product: woocommerce_shipping					
Affected Version(s): * Up to (including) 1.2.11					
Missing Authorization	12-Dec-2022	8.1	The WooCommerce Shipping WordPress plugin through 1.2.11 does not have authorisation and CRSF in an AJAX action, which could allow any authenticated users, such as subscriber to delete arbitrary options from the blog, which could make the blog unavailable. **CVE ID : CVE-2022-3999**	N/A	A-DPD-WOOC-191222/156
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	4.8	The WooCommerce Shipping WordPress plugin through 1.2.11 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).	N/A	A-DPD-WOOC-191222/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-4000		
Vendor: ecommerce-website_project					
Product: ecommerce-website					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the component /signup_script.php of Ecommerce-Website v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the eMail parameter. **CVE ID : CVE-2022-45990**	N/A	A-ECO-ECOM-191222/158
Vendor: elbtide					
Product: advanced_booking_calendar					
Affected Version(s): * Up to (including) 1.7.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Dec-2022	9.8	Unauth. SQL Injection (SQLi) vulnerability in Advanced Booking Calendar plugin <= 1.7.1 on WordPress. **CVE ID : CVE-2022-45822**	N/A	A-ELB-ADVA-191222/159
Cross-Site Request Forgery (CSRF)	05-Dec-2022	6.5	Cross-Site Request Forgery (CSRF) vulnerability in Advanced Booking Calendar plugin <= 1.7.1 on WordPress. **CVE ID : CVE-2022-45824**	N/A	A-ELB-ADVA-191222/160
Vendor: enhancesoft					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: osticket					
Affected Version(s): * Up to (excluding) 1.16.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	5.4	Cross-site Scripting (XSS) - Reflected in GitHub repository osticket/osticket prior to 1.16.4. **CVE ID : CVE-2022-4271**	https://huntr.dev/bounties/a11c922f-255a-412a-aa87-7f3bd7121599, https://github.com/osticket/osticket/commit/5213ff138c6be6144a6692376ac0803a42eca168	A-ENH-OSTI-191222/161
Vendor: F5					
Product: big-ip_access_policy_manager					
Affected Version(s): 17.0.0					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/162
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/164
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**		
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/166
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/167
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.8					
Cross-Site Request	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are	https://support.f5.com/csp	A-F5-BIG--191222/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	/article/K94221585	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/169
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.3					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41622		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/171
Product: big-ip_advanced_firewall_manager					
Affected Version(s): 17.0.0					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/172
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cross-Site Request	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site	https://support.f5.com/csp	A-F5-BIG--191222/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	/article/K94221585	
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/174
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.8					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/175
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.3					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**		
Affected Version(s): From (including) 13.1.0 Up to (including) 17.0.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/177
Product: big-ip_analytics					
Affected Version(s): 17.0.0					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41622		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/179
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/180
Improper Neutralization of Special Elements used in a	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**		
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/182
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.8					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/184
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.3					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/186
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/187
Product: big-ip_application_acceleration_manager					
Affected Version(s): 17.0.0					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/189
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/191
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/192
Improper Neutralization of Special Elements used in a Command ('Comman	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.8					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/194
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**		
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.3					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/196
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/197
Product: big-ip_application_security_manager					
Affected Version(s): 17.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/198
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/199
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/201
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/202
Improper Neutralization of Special	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user	https://support.f5.com/csp	A-F5-BIG--191222/203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	/article/K13325942	
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.8					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/204
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**		
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.3					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/206
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41800		
Product: big-ip_domain_name_system					
Affected Version(s): 17.0.0					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/208
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/209
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cross-Site Request	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site	https://support.f5.com/csp	A-F5-BIG--191222/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	/article/K94221585	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/211
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41622		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/213
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.8					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/214
Improper Neutralization of Special Elements used in a	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**		
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.3					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/216
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**		
Product: big-ip_fraud_protection_service					
Affected Version(s): 17.0.0					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/218
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41800		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/220
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/221
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/223
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.8					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/225
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.3					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/226
Improper Neutralization of Special Elements used in a Command ('Comman	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**		
Product: big-ip_global_traffic_manager					
Affected Version(s): 17.0.0					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/228
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note:	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/230
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/231
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/232
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/233
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.8					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/235
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.3					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/236
Improper Neutralization of Special	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user	https://support.f5.com/csp	A-F5-BIG--191222/237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	/article/K13325942	
Product: big-ip_link_controller					
Affected Version(s): 17.0.0					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/238
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/240
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41800		
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/242
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/243
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.8					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/245
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.3					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/247
Product: big-ip_local_traffic_manager					
Affected Version(s): 17.0.0					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/248
Improper Neutralization of Special Elements used in a Command	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/250
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note:	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**		
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/252
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/253
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/254
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/255
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.3					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/257
Product: big-ip_policy_enforcement_manager					
Affected Version(s): 17.0.0					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/258
Improper Neutralizat	07-Dec-2022	8.7	In all versions of BIG-IP, when running in	https://support.f5.com/csp	A-F5-BIG--191222/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	/article/K13325942	
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/260
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**		
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/262
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.8					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/264
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/265
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.3					
Cross-Site Request	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are	https://support.f5.com/csp	A-F5-BIG--191222/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	/article/K94221585	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	8.7	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41800**	https://support.f5.com/csp/article/K13325942	A-F5-BIG--191222/267
Product: big-iq_centralized_management					
Affected Version(s): 7.1.0					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**		
Affected Version(s): From (including) 8.0.0 Up to (including) 8.2.0					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-41622**	https://support.f5.com/csp/article/K94221585	A-F5-BIG--191222/269
Vendor: facepay_project					
Product: facepay					
Affected Version(s): 1.0					
Improper Authorization	05-Dec-2022	8.8	A vulnerability has been found in Facepay 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /face-recognition-php/facepay-master/camera.php. The manipulation of the argument userId leads to authorization bypass. The attack can be launched remotely. The identifier VDB-214789 was assigned to this vulnerability. **CVE ID : CVE-2022-4281**	N/A	A-FAC-FACE-191222/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Fedoraproject					
Product: extra_packages_for_enterprise_linux					
Affected Version(s): 8.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	09-Dec-2022	9.8	The rxvt-unicode package is vulnerable to a remote code execution, in the Perl background extension, when an attacker can control the data written to the user's terminal and certain options are set. **CVE ID : CVE-2022-4170**	N/A	A-FED-EXTR-191222/271
Vendor: ff4j					
Product: ff4j					
Affected Version(s): 1.8.1					
N/A	01-Dec-2022	9.8	ff4j 1.8.1 is vulnerable to Remote Code Execution (RCE). **CVE ID : CVE-2022-44262**	N/A	A-FF4-FF4J-191222/272
Vendor: Fortinet					
Product: fortiadc					
Affected Version(s): 7.1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Dec-2022	8.8	An improper neutralization of special elements used in an SQL Command ('SQL Injection') vulnerability in Fortinet FortiADC version 7.1.0, version 7.0.0 through 7.0.2 and version 6.2.4 and below allows an authenticated attacker to execute unauthorized code or commands via	https://fortiguard.com/psirt/FG-IR-22-252	A-FOR-FORT-191222/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specifically crafted HTTP requests. **CVE ID : CVE-2022-33875**		
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	06-Dec-2022	6.5	Multiple instances of improper input validation vulnerability in Fortinet FortiADC version 7.1.0, version 7.0.0 through 7.0.2 and version 6.2.4 and below allows an authenticated attacker to retrieve files with specific extension from the underlying Linux system via crafted HTTP requests. **CVE ID : CVE-2022-33876**	https://fortiguard.com/psirt/FG-IR-22-253	A-FOR-FORT-191222/274
Affected Version(s): 7.0.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Dec-2022	8.8	An improper neutralization of special elements used in an SQL Command ('SQL Injection') vulnerability in Fortinet FortiADC version 7.1.0, version 7.0.0 through 7.0.2 and version 6.2.4 and below allows an authenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests. **CVE ID : CVE-2022-33875**	https://fortiguard.com/psirt/FG-IR-22-252	A-FOR-FORT-191222/275
Inconsistent Interpretation of HTTP	06-Dec-2022	6.5	Multiple instances of improper input validation vulnerability in Fortinet FortiADC version 7.1.0, version	https://fortiguard.com/psirt/FG-IR-22-253	A-FOR-FORT-191222/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Requests ('HTTP Request Smuggling')			7.0.0 through 7.0.2 and version 6.2.4 and below allows an authenticated attacker to retrieve files with specific extension from the underlying Linux system via crafted HTTP requests. **CVE ID : CVE-2022-33876**		
Affected Version(s): 7.0.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Dec-2022	8.8	An improper neutralization of special elements used in an SQL Command ('SQL Injection') vulnerability in Fortinet FortiADC version 7.1.0, version 7.0.0 through 7.0.2 and version 6.2.4 and below allows an authenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests. **CVE ID : CVE-2022-33875**	https://fortiguard.com/psirt/FG-IR-22-252	A-FOR-FORT-191222/277
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	06-Dec-2022	6.5	Multiple instances of improper input validation vulnerability in Fortinet FortiADC version 7.1.0, version 7.0.0 through 7.0.2 and version 6.2.4 and below allows an authenticated attacker to retrieve files with specific extension from the underlying Linux system via crafted HTTP requests.	https://fortiguard.com/psirt/FG-IR-22-253	A-FOR-FORT-191222/278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33876		
Affected Version(s): 7.0.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Dec-2022	8.8	An improper neutralization of special elements used in an SQL Command ('SQL Injection') vulnerability in Fortinet FortiADC version 7.1.0, version 7.0.0 through 7.0.2 and version 6.2.4 and below allows an authenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests. **CVE ID : CVE-2022-33875**	https://fortiguard.com/psirt/FG-IR-22-252	A-FOR-FORT-191222/279
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	06-Dec-2022	6.5	Multiple instances of improper input validation vulnerability in Fortinet FortiADC version 7.1.0, version 7.0.0 through 7.0.2 and version 6.2.4 and below allows an authenticated attacker to retrieve files with specific extension from the underlying Linux system via crafted HTTP requests. **CVE ID : CVE-2022-33876**	https://fortiguard.com/psirt/FG-IR-22-253	A-FOR-FORT-191222/280
Affected Version(s): From (including) 5.1.0 Up to (including) 6.2.4					
Inconsistent Interpretation of HTTP Requests	06-Dec-2022	6.5	Multiple instances of improper input validation vulnerability in Fortinet FortiADC version 7.1.0, version 7.0.0 through 7.0.2 and	https://fortiguard.com/psirt/FG-IR-22-253	A-FOR-FORT-191222/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('HTTP Request Smuggling')			version 6.2.4 and below allows an authenticated attacker to retrieve files with specific extension from the underlying Linux system via crafted HTTP requests. **CVE ID : CVE-2022-33876**		
Affected Version(s): From (including) 5.2.0 Up to (including) 6.2.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Dec-2022	8.8	An improper neutralization of special elements used in an SQL Command ('SQL Injection') vulnerability in Fortinet FortiADC version 7.1.0, version 7.0.0 through 7.0.2 and version 6.2.4 and below allows an authenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests. **CVE ID : CVE-2022-33875**	https://fortiguard.com/psirt/FG-IR-22-252	A-FOR-FORT-191222/282
Product: fortideceptor					
Affected Version(s): 3.1.0					
N/A	06-Dec-2022	7.5	An insufficient logging [CWE-778] vulnerability in FortiSandbox versions 4.0.0 to 4.0.2, 3.2.0 to 3.2.3 and 3.1.0 to 3.1.5 and FortiDeceptor versions 4.2.0, 4.1.0 through 4.1.1, 4.0.0 through 4.0.2, 3.3.0 through 3.3.3, 3.2.0 through 3.2.2,3.1.0 through 3.1.1 and 3.0.0 through 3.0.2 may allow	https://fortiguard.com/psirt/FG-IR-21-170	A-FOR-FORT-191222/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a remote attacker to repeatedly enter incorrect credentials without causing a log entry, and with no limit on the number of failed authentication attempts. **CVE ID : CVE-2022-30305**		
Affected Version(s): 3.1.1					
N/A	06-Dec-2022	7.5	An insufficient logging [CWE-778] vulnerability in FortiSandbox versions 4.0.0 to 4.0.2, 3.2.0 to 3.2.3 and 3.1.0 to 3.1.5 and FortiDeceptor versions 4.2.0, 4.1.0 through 4.1.1, 4.0.0 through 4.0.2, 3.3.0 through 3.3.3, 3.2.0 through 3.2.2,3.1.0 through 3.1.1 and 3.0.0 through 3.0.2 may allow a remote attacker to repeatedly enter incorrect credentials without causing a log entry, and with no limit on the number of failed authentication attempts. **CVE ID : CVE-2022-30305**	https://fortiguard.com/psirt/FG-IR-21-170	A-FOR-FORT-191222/284
Affected Version(s): 4.1.0					
N/A	06-Dec-2022	7.5	An insufficient logging [CWE-778] vulnerability in FortiSandbox versions 4.0.0 to 4.0.2, 3.2.0 to 3.2.3 and 3.1.0 to 3.1.5 and FortiDeceptor versions 4.2.0, 4.1.0 through 4.1.1, 4.0.0 through 4.0.2, 3.3.0	https://fortiguard.com/psirt/FG-IR-21-170	A-FOR-FORT-191222/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 3.3.3, 3.2.0 through 3.2.2,3.1.0 through 3.1.1 and 3.0.0 through 3.0.2 may allow a remote attacker to repeatedly enter incorrect credentials without causing a log entry, and with no limit on the number of failed authentication attempts. **CVE ID : CVE-2022-30305**		
Affected Version(s): 4.1.1					
N/A	06-Dec-2022	7.5	An insufficient logging [CWE-778] vulnerability in FortiSandbox versions 4.0.0 to 4.0.2, 3.2.0 to 3.2.3 and 3.1.0 to 3.1.5 and FortiDeceptor versions 4.2.0, 4.1.0 through 4.1.1, 4.0.0 through 4.0.2, 3.3.0 through 3.3.3, 3.2.0 through 3.2.2,3.1.0 through 3.1.1 and 3.0.0 through 3.0.2 may allow a remote attacker to repeatedly enter incorrect credentials without causing a log entry, and with no limit on the number of failed authentication attempts. **CVE ID : CVE-2022-30305**	https://fortiguard.com/psirt/FG-IR-21-170	A-FOR-FORT-191222/286
Affected Version(s): 4.2.0					
N/A	06-Dec-2022	7.5	An insufficient logging [CWE-778] vulnerability in FortiSandbox versions 4.0.0 to 4.0.2, 3.2.0 to 3.2.3 and 3.1.0 to 3.1.5	https://fortiguard.com/psirt/FG-IR-21-170	A-FOR-FORT-191222/287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and FortiDeceptor versions 4.2.0, 4.1.0 through 4.1.1, 4.0.0 through 4.0.2, 3.3.0 through 3.3.3, 3.2.0 through 3.2.2,3.1.0 through 3.1.1 and 3.0.0 through 3.0.2 may allow a remote attacker to repeatedly enter incorrect credentials without causing a log entry, and with no limit on the number of failed authentication attempts. **CVE ID : CVE-2022-30305**		
Affected Version(s): From (including) 3.0.0 Up to (including) 3.0.2					
N/A	06-Dec-2022	7.5	An insufficient logging [CWE-778] vulnerability in FortiSandbox versions 4.0.0 to 4.0.2, 3.2.0 to 3.2.3 and 3.1.0 to 3.1.5 and FortiDeceptor versions 4.2.0, 4.1.0 through 4.1.1, 4.0.0 through 4.0.2, 3.3.0 through 3.3.3, 3.2.0 through 3.2.2,3.1.0 through 3.1.1 and 3.0.0 through 3.0.2 may allow a remote attacker to repeatedly enter incorrect credentials without causing a log entry, and with no limit on the number of failed authentication attempts. **CVE ID : CVE-2022-30305**	https://fortiguard.com/psirt/FG-IR-21-170	A-FOR-FORT-191222/288
Affected Version(s): From (including) 3.2.0 Up to (including) 3.2.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Dec-2022	7.5	An insufficient logging [CWE-778] vulnerability in FortiSandbox versions 4.0.0 to 4.0.2, 3.2.0 to 3.2.3 and 3.1.0 to 3.1.5 and FortiDeceptor versions 4.2.0, 4.1.0 through 4.1.1, 4.0.0 through 4.0.2, 3.3.0 through 3.3.3, 3.2.0 through 3.2.2,3.1.0 through 3.1.1 and 3.0.0 through 3.0.2 may allow a remote attacker to repeatedly enter incorrect credentials without causing a log entry, and with no limit on the number of failed authentication attempts. **CVE ID : CVE-2022-30305**	https://fortiguard.com/psirt/FG-IR-21-170	A-FOR-FORT-191222/289
Affected Version(s): From (including) 3.3.0 Up to (including) 3.3.3					
N/A	06-Dec-2022	7.5	An insufficient logging [CWE-778] vulnerability in FortiSandbox versions 4.0.0 to 4.0.2, 3.2.0 to 3.2.3 and 3.1.0 to 3.1.5 and FortiDeceptor versions 4.2.0, 4.1.0 through 4.1.1, 4.0.0 through 4.0.2, 3.3.0 through 3.3.3, 3.2.0 through 3.2.2,3.1.0 through 3.1.1 and 3.0.0 through 3.0.2 may allow a remote attacker to repeatedly enter incorrect credentials without causing a log entry, and with no limit on the number of failed authentication attempts.	https://fortiguard.com/psirt/FG-IR-21-170	A-FOR-FORT-191222/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30305		
Affected Version(s): From (including) 4.0.0 Up to (including) 4.0.2					
N/A	06-Dec-2022	7.5	An insufficient logging [CWE-778] vulnerability in FortiSandbox versions 4.0.0 to 4.0.2, 3.2.0 to 3.2.3 and 3.1.0 to 3.1.5 and FortiDeceptor versions 4.2.0, 4.1.0 through 4.1.1, 4.0.0 through 4.0.2, 3.3.0 through 3.3.3, 3.2.0 through 3.2.2,3.1.0 through 3.1.1 and 3.0.0 through 3.0.2 may allow a remote attacker to repeatedly enter incorrect credentials without causing a log entry, and with no limit on the number of failed authentication attempts. **CVE ID : CVE-2022-30305**	https://fortiguard.com/psirt/FG-IR-21-170	A-FOR-FORT-191222/291
Product: fortiproxy					
Affected Version(s): From (including) 1.2.0 Up to (including) 1.2.13					
N/A	06-Dec-2022	9.8	An authentication bypass by assumed-immutable data vulnerability [CWE-302] in the FortiOS SSH login component 7.2.0, 7.0.0 through 7.0.7, 6.4.0 through 6.4.9, 6.2 all versions, 6.0 all versions and FortiProxy SSH login component 7.0.0 through 7.0.5, 2.0.0 through 2.0.10, 1.2.0 all versions may allow a remote and unauthenticated attacker to login into the device	https://fortiguard.com/psirt/FG-IR-22-255	A-FOR-FORT-191222/292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via sending specially crafted Access-Challenge response from the Radius server. **CVE ID : CVE-2022-35843**		
Affected Version(s): From (including) 2.0.0 Up to (including) 2.0.10					
N/A	06-Dec-2022	9.8	An authentication bypass by assumed-immutable data vulnerability [CWE-302] in the FortiOS SSH login component 7.2.0, 7.0.0 through 7.0.7, 6.4.0 through 6.4.9, 6.2 all versions, 6.0 all versions and FortiProxy SSH login component 7.0.0 through 7.0.5, 2.0.0 through 2.0.10, 1.2.0 all versions may allow a remote and unauthenticated attacker to login into the device via sending specially crafted Access-Challenge response from the Radius server. **CVE ID : CVE-2022-35843**	https://fortiguard.com/psirt/FG-IR-22-255	A-FOR-FORT-191222/293
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.6					
N/A	06-Dec-2022	9.8	An authentication bypass by assumed-immutable data vulnerability [CWE-302] in the FortiOS SSH login component 7.2.0, 7.0.0 through 7.0.7, 6.4.0 through 6.4.9, 6.2 all versions, 6.0 all versions and FortiProxy SSH login component 7.0.0 through 7.0.5, 2.0.0 through 2.0.10, 1.2.0 all versions may allow a remote and	https://fortiguard.com/psirt/FG-IR-22-255	A-FOR-FORT-191222/294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to login into the device via sending specially crafted Access-Challenge response from the Radius server. **CVE ID : CVE-2022-35843**		
Product: fortisandbox					
Affected Version(s): From (including) 4.0.0 Up to (including) 4.0.2					
N/A	06-Dec-2022	7.5	An insufficient logging [CWE-778] vulnerability in FortiSandbox versions 4.0.0 to 4.0.2, 3.2.0 to 3.2.3 and 3.1.0 to 3.1.5 and FortiDeceptor versions 4.2.0, 4.1.0 through 4.1.1, 4.0.0 through 4.0.2, 3.3.0 through 3.3.3, 3.2.0 through 3.2.2,3.1.0 through 3.1.1 and 3.0.0 through 3.0.2 may allow a remote attacker to repeatedly enter incorrect credentials without causing a log entry, and with no limit on the number of failed authentication attempts. **CVE ID : CVE-2022-30305**	https://fortiguard.com/psirt/FG-IR-21-170	A-FOR-FORT-191222/295
Affected Version(s): 3.2.0					
N/A	06-Dec-2022	7.5	An insufficient logging [CWE-778] vulnerability in FortiSandbox versions 4.0.0 to 4.0.2, 3.2.0 to 3.2.3 and 3.1.0 to 3.1.5 and FortiDeceptor versions 4.2.0, 4.1.0 through 4.1.1, 4.0.0 through 4.0.2, 3.3.0	https://fortiguard.com/psirt/FG-IR-21-170	A-FOR-FORT-191222/296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 3.3.3, 3.2.0 through 3.2.2,3.1.0 through 3.1.1 and 3.0.0 through 3.0.2 may allow a remote attacker to repeatedly enter incorrect credentials without causing a log entry, and with no limit on the number of failed authentication attempts. **CVE ID : CVE-2022-30305**		
Affected Version(s): 3.2.1					
N/A	06-Dec-2022	7.5	An insufficient logging [CWE-778] vulnerability in FortiSandbox versions 4.0.0 to 4.0.2, 3.2.0 to 3.2.3 and 3.1.0 to 3.1.5 and FortiDeceptor versions 4.2.0, 4.1.0 through 4.1.1, 4.0.0 through 4.0.2, 3.3.0 through 3.3.3, 3.2.0 through 3.2.2,3.1.0 through 3.1.1 and 3.0.0 through 3.0.2 may allow a remote attacker to repeatedly enter incorrect credentials without causing a log entry, and with no limit on the number of failed authentication attempts. **CVE ID : CVE-2022-30305**	https://fortiguard.com/psirt/FG-IR-21-170	A-FOR-FORT-191222/297
Affected Version(s): 3.2.2					
N/A	06-Dec-2022	7.5	An insufficient logging [CWE-778] vulnerability in FortiSandbox versions 4.0.0 to 4.0.2, 3.2.0 to 3.2.3 and 3.1.0 to 3.1.5	https://fortiguard.com/psirt/FG-IR-21-170	A-FOR-FORT-191222/298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and FortiDeceptor versions 4.2.0, 4.1.0 through 4.1.1, 4.0.0 through 4.0.2, 3.3.0 through 3.3.3, 3.2.0 through 3.2.2,3.1.0 through 3.1.1 and 3.0.0 through 3.0.2 may allow a remote attacker to repeatedly enter incorrect credentials without causing a log entry, and with no limit on the number of failed authentication attempts. **CVE ID : CVE-2022-30305**		
Affected Version(s): 3.2.3					
N/A	06-Dec-2022	7.5	An insufficient logging [CWE-778] vulnerability in FortiSandbox versions 4.0.0 to 4.0.2, 3.2.0 to 3.2.3 and 3.1.0 to 3.1.5 and FortiDeceptor versions 4.2.0, 4.1.0 through 4.1.1, 4.0.0 through 4.0.2, 3.3.0 through 3.3.3, 3.2.0 through 3.2.2,3.1.0 through 3.1.1 and 3.0.0 through 3.0.2 may allow a remote attacker to repeatedly enter incorrect credentials without causing a log entry, and with no limit on the number of failed authentication attempts. **CVE ID : CVE-2022-30305**	https://fortiguard.com/psirt/FG-IR-21-170	A-FOR-FORT-191222/299
Affected Version(s): From (including) 3.1.0 Up to (including) 3.1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Dec-2022	7.5	An insufficient logging [CWE-778] vulnerability in FortiSandbox versions 4.0.0 to 4.0.2, 3.2.0 to 3.2.3 and 3.1.0 to 3.1.5 and FortiDeceptor versions 4.2.0, 4.1.0 through 4.1.1, 4.0.0 through 4.0.2, 3.3.0 through 3.3.3, 3.2.0 through 3.2.2,3.1.0 through 3.1.1 and 3.0.0 through 3.0.2 may allow a remote attacker to repeatedly enter incorrect credentials without causing a log entry, and with no limit on the number of failed authentication attempts. **CVE ID : CVE-2022-30305**	https://fortiguard.com/psirt/FG-IR-21-170	A-FOR-FORT-191222/300
Product: fortisoar					
Affected Version(s): 7.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	5.4	Improper neutralization of input during web page generation [CWE-79] in FortiSOAR 7.0.0 through 7.0.3 and 7.2.0 may allow an authenticated attacker to inject HTML tags via input fields of various components within FortiSOAR. **CVE ID : CVE-2022-38379**	https://fortiguard.com/psirt/FG-IR-22-220	A-FOR-FORT-191222/301
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.3					
Improper Neutralization of Input During	06-Dec-2022	5.4	Improper neutralization of input during web page generation [CWE-79] in FortiSOAR 7.0.0 through 7.0.3 and 7.2.0 may allow	https://fortiguard.com/psirt/FG-IR-22-220	A-FOR-FORT-191222/302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			an authenticated attacker to inject HTML tags via input fields of various components within FortiSOAR. **CVE ID : CVE-2022-38379**		
Vendor: freshrss					
Product: freshrss					
Affected Version(s): From (including) 1.18.0 Up to (excluding) 1.20.2					
Exposure of Sensitive Information to an Unauthorized Actor	09-Dec-2022	7.5	FreshRSS is a free, self-hostable RSS aggregator. User configuration files can be accessed by a remote user. In addition to user preferences, such configurations contain hashed passwords (brypt with cost 9, salted) of FreshRSS Web interface. If the API is used, the configuration might contain a hashed password (brypt with cost 9, salted) of the GReader API, and a hashed password (MD5 salted) of the Fever API. Users should update to version 1.20.2 or edge. Users unable to upgrade can apply the patch manually or delete the file `./FreshRSS/p/ext.php`. **CVE ID : CVE-2022-23497**	https://github.com/FreshRSS/FreshRSS/pull/4928, https://github.com/FreshRSS/FreshRSS/releases/tag/1.20.2	A-FRE-FRES-191222/303
Vendor: fs-blog_project					
Product: fs-blog					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Dec-2022	6.1	A vulnerability was found in zbl1996 FS-Blog and classified as problematic. This issue affects some unknown processing of the component Title Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-215267. **CVE ID : CVE-2022-4400**	N/A	A-FS--FS-B-191222/304
Vendor: funkwhale					
Product: funkwhale					
Affected Version(s): 1.2.8					
Operation on a Resource after Expiration or Release	09-Dec-2022	5.3	User invites for Funkwhale v1.2.8 do not permanently expire after being used for signup and can be used again after an account has been deleted. **CVE ID : CVE-2022-45292**	https://dev.funkwhale.audio/funkwhale/funkwhale/-/issues/1952	A-FUN-FUNK-191222/305
Vendor: g5theme					
Product: essential_real_estate					
Affected Version(s): * Up to (excluding) 3.9.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	5.4	The Essential Real Estate WordPress plugin before 3.9.6 does not sanitize and escapes some parameters, which could allow users with a role as low as Admin to perform Cross-Site Scripting attacks.	N/A	A-G5T-ESSE-191222/306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3933		
Vendor: galaxyproject					
Product: galaxy					
Affected Version(s): From (including) 22.01 Up to (including) 22.05					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Dec-2022	7.5	Galaxy is an open-source platform for data analysis. An arbitrary file read exists in Galaxy 22.01 and Galaxy 22.05 due to the switch to Gunicorn, which can be used to read any file accessible to the operating system user under which Galaxy is running. This vulnerability affects Galaxy 22.01 and higher, after the switch to gunicorn, which serve static contents directly. Additionally, the vulnerability is mitigated when using Nginx or Apache to serve /static/* contents, instead of Galaxy's internal middleware. This issue has been patched in commit `e5e6bda4f` and will be included in future releases. Users are advised to manually patch their installations. There are no known workarounds for this vulnerability. **CVE ID : CVE-2022-23470**	https://github.com/galaxyproject/galaxy/security/advisories/GHSA-grjf-2ghx-q77x, https://github.com/galaxyproject/galaxy/commit/e5e6bda4f014f807ca77ee0cf6af777a55918346	A-GAL-GALA-191222/307
Vendor: GE					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: cimplicity					
Affected Version(s): * Up to (including) 2022					
Untrusted Pointer Dereference	07-Dec-2022	7.8	GE CIMPICITY versions 2022 and prior is vulnerable when data from faulting address controls code flow starting at gmmiObj!CGmmiOptionContainer, which could allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-2002**	N/A	A-GE-CIMP-191222/308
Heap-based Buffer Overflow	07-Dec-2022	7.8	GE CIMPICITY versions 2022 and prior is vulnerable to a heap-based buffer overflow, which could allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-2948**	N/A	A-GE-CIMP-191222/309
Access of Uninitialized Pointer	07-Dec-2022	7.8	GE CIMPICITY versions 2022 and prior is vulnerable when data from a faulting address controls code flow starting at gmmiObj!CGmmiOptionContainer, which could allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-2952**	N/A	A-GE-CIMP-191222/310
Access of Uninitialized Pointer	08-Dec-2022	7.8	GE CIMPICITY versions 2022 and prior is vulnerable when data from a faulting address controls code flow starting at	N/A	A-GE-CIMP-191222/311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gmmiObj!CGmmiRootOptionTable, which could allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3084**		
Out-of-bounds Write	08-Dec-2022	7.8	GE CIMPICITY versions 2022 and prior is vulnerable to an out-of-bounds write, which could allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3092**	N/A	A-GE-CIMP-191222/312
Vendor: getyourguide_ticketing_project					
Product: getyourguide_ticketing					
Affected Version(s): * Up to (excluding) 1.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	4.8	The GetYourGuide Ticketing WordPress plugin before 1.0.4 does not sanitise and escape some parameters, 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-2022-3609**	N/A	A-GET-GETY-191222/313
Vendor: gitea					
Product: gitea					
Affected Version(s): * Up to (excluding) 1.4.5					
Cleartext Transmission of Sensitive	12-Dec-2022	4.3	In Jenkins Gitea Plugin 1.4.4 and earlier, the implementation of Gitea personal access tokens	https://www.jenkins.io/security/advisory/2022-12-	A-GIT-GITE-191222/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			did not support credentials masking, potentially exposing them through the build log. **CVE ID : CVE-2022-46685**	07/#SECURITY-2661	
Vendor: Github					
Product: enterprise_server					
Affected Version(s): * Up to (excluding) 3.2.20					
Improper Privilege Management	01-Dec-2022	6.5	An improper privilege management vulnerability was identified in GitHub Enterprise Server that allowed users with improper privileges to create or delete pages via the API. To exploit this vulnerability, an attacker would need to be added to an organization's repo with write permissions. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.7 and was fixed in versions 3.2.20, 3.3.15, 3.4.10, 3.5.7, and 3.6.3. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2022-23737**	https://docs.github.com/en/enterprise-server@3.2/admin/release-notes#3.2.20, https://docs.github.com/en/enterprise-server@3.3/admin/release-notes#3.3.15, https://docs.github.com/en/enterprise-server@3.4/admin/release-notes#3.4.10	A-GIT-ENTE-191222/315
Affected Version(s): From (including) 3.3.0 Up to (excluding) 3.3.15					
Improper Privilege Management	01-Dec-2022	6.5	An improper privilege management vulnerability was identified in GitHub Enterprise Server that allowed users with	https://docs.github.com/en/enterprise-server@3.2/admin/release-notes#3.2.20,	A-GIT-ENTE-191222/316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper privileges to create or delete pages via the API. To exploit this vulnerability, an attacker would need to be added to an organization's repo with write permissions. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.7 and was fixed in versions 3.2.20, 3.3.15, 3.4.10, 3.5.7, and 3.6.3. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2022-23737**	https://docs.github.com/en/enterprise-server@3.3/admin/release-notes#3.3.15, https://docs.github.com/en/enterprise-server@3.4/admin/release-notes#3.4.10	
Affected Version(s): From (including) 3.4.0 Up to (excluding) 3.4.10					
Improper Privilege Management	01-Dec-2022	6.5	An improper privilege management vulnerability was identified in GitHub Enterprise Server that allowed users with improper privileges to create or delete pages via the API. To exploit this vulnerability, an attacker would need to be added to an organization's repo with write permissions. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.7 and was fixed in versions 3.2.20, 3.3.15, 3.4.10, 3.5.7, and 3.6.3. This vulnerability was reported via the GitHub Bug Bounty program.	https://docs.github.com/en/enterprise-server@3.2/admin/release-notes#3.2.20, https://docs.github.com/en/enterprise-server@3.3/admin/release-notes#3.3.15, https://docs.github.com/en/enterprise-server@3.4/admin/release-notes#3.4.10	A-GIT-ENTE-191222/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23737		
Affected Version(s): From (including) 3.5.0 Up to (excluding) 3.5.7					
Improper Privilege Management	01-Dec-2022	6.5	An improper privilege management vulnerability was identified in GitHub Enterprise Server that allowed users with improper privileges to create or delete pages via the API. To exploit this vulnerability, an attacker would need to be added to an organization's repo with write permissions. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.7 and was fixed in versions 3.2.20, 3.3.15, 3.4.10, 3.5.7, and 3.6.3. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2022-23737**	https://docs.github.com/en/enterprise-server@3.2/admin/release-notes#3.2.20, https://docs.github.com/en/enterprise-server@3.3/admin/release-notes#3.3.15, https://docs.github.com/en/enterprise-server@3.4/admin/release-notes#3.4.10	A-GIT-ENTE-191222/318
Affected Version(s): From (including) 3.6.0 Up to (excluding) 3.6.3					
Improper Privilege Management	01-Dec-2022	6.5	An improper privilege management vulnerability was identified in GitHub Enterprise Server that allowed users with improper privileges to create or delete pages via the API. To exploit this vulnerability, an attacker would need to be added to an organization's repo with write permissions. This vulnerability	https://docs.github.com/en/enterprise-server@3.2/admin/release-notes#3.2.20, https://docs.github.com/en/enterprise-server@3.3/admin/release-notes#3.3.15, https://docs.github.com/en	A-GIT-ENTE-191222/319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected all versions of GitHub Enterprise Server prior to 3.7 and was fixed in versions 3.2.20, 3.3.15, 3.4.10, 3.5.7, and 3.6.3. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2022-23737**	/enterprise-server@3.4/admin/release-notes#3.4.10	
Vendor: gitpython_project					
Product: gitpython					
Affected Version(s): -					
Improper Input Validation	06-Dec-2022	9.8	All versions of package gitpython are vulnerable to Remote Code Execution (RCE) due to improper user input validation, which makes it possible to inject a maliciously crafted remote URL into the clone command. Exploiting this vulnerability is possible because the library makes external calls to git without sufficient sanitization of input arguments. **CVE ID : CVE-2022-24439**	https://security.snyk.io/vuln/SNYK-PYTHON-GITPYTHON-3113858, https://github.com/gitpython-developers/GitPython/blob/bec61576ae75803bc4e60d8de7a629c194313d1c/git/repo/base.py%23L1249	A-GIT-GITP-191222/320
Vendor: gl-inet					
Product: goodcloud					
Affected Version(s): * Up to (including) 1.0					
N/A	01-Dec-2022	7.4	In GL.iNet Goodcloud 1.1 Incorrect access control allows a remote attacker to access/change devices' settings.	https://forum.gl-inet.com/t/security-advisories-vulnerabilities	A-GL--GOOD-191222/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-44211	-and-cves-of-gl-inet-software/25518	
N/A	01-Dec-2022	5.9	In GL.iNet Goodcloud 1.0, insecure design allows remote attacker to access devices' admin panel. **CVE ID : CVE-2022-44212**	N/A	A-GL--GOOD-191222/322
Vendor: goauthentik					
Product: authentik					
Affected Version(s): * Up to (excluding) 2022.10.2					
Improper Authentication	02-Dec-2022	9.8	authentik is an open-source identity provider. Versions prior to 2022.11.2 and 2022.10.2 are vulnerable to unauthorized user creation and potential account takeover. With the default flows, unauthenticated users can create new accounts in authentik. If a flow exists that allows for email-verified password recovery, this can be used to overwrite the email address of admin accounts and take over their accounts. authentik 2022.11.2 and 2022.10.2 fix this issue. As a workaround, a policy can be created and bound to the `default-user-settings-flow flow` with the contents `return request.user.is_authenticated`.	https://goauthentik.io/docs/releases/2022.11#fixed-in-2022112, https://goauthentik.io/docs/releases/2022.10#fixed-in-2022102	A-GOA-AUTH-191222/323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46145		
Affected Version(s): From (including) 2022.11 Up to (excluding) 2022.11.2					
Improper Authentication	02-Dec-2022	9.8	authentik is an open-source identity provider. Versions prior to 2022.11.2 and 2022.10.2 are vulnerable to unauthorized user creation and potential account takeover. With the default flows, unauthenticated users can create new accounts in authentik. If a flow exists that allows for email-verified password recovery, this can be used to overwrite the email address of admin accounts and take over their accounts. authentik 2022.11.2 and 2022.10.2 fix this issue. As a workaround, a policy can be created and bound to the `default-user-settings-flow flow` with the contents `return request.user.is_authenticated`. **CVE ID : CVE-2022-46145**	https://goauthentik.io/docs/releases/2022.11#fixed-in-2022112, https://goauthentik.io/docs/releases/2022.10#fixed-in-2022102	A-GOA-AUTH-191222/324
Vendor: Golang					
Product: go					
Affected Version(s): * Up to (excluding) 1.18.9					
Improper Limitation of a Pathname to a Restricted	07-Dec-2022	7.5	On Windows, restricted files can be accessed via os.DirFS and http.Dir. The os.DirFS function and http.Dir type provide access to a tree of files	https://groups.google.com/g/golang-announce/c/L_3rmdT0BMU/m/yZDrXjIiB	A-GOL-GO-191222/325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			rooted at a given directory. These functions permit access to Windows device files under that root. For example, os.DirFS("C:/tmp").Open ("COM1") opens the COM1 device. Both os.DirFS and http.Dir only provide read-only filesystem access. In addition, on Windows, an os.DirFS for the directory (the root of the current drive) can permit a maliciously crafted path to escape from the drive and access any path on the system. With fix applied, the behavior of os.DirFS("") has changed. Previously, an empty root was treated equivalently to "/", so os.DirFS("").Open("tmp") would open the path "/tmp". This now returns an error. **CVE ID : CVE-2022-41720**	QAJ, https://pkg.go.dev/vuln/GO-2022-1143, https://go.dev/cl/455716, https://go.dev/issue/56694	
Allocation of Resources Without Limits or Throttling	08-Dec-2022	5.3	An attacker can cause excessive memory growth in a Go server accepting HTTP/2 requests. HTTP/2 server connections contain a cache of HTTP header keys sent by the client. While the total number of entries in this cache is capped, an attacker sending very large keys	https://pkg.go.dev/vuln/GO-2022-1144, https://go.dev/cl/455717, https://go.dev/issue/56350, https://go.dev/cl/455635	A-GOL-GO-191222/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause the server to allocate approximately 64 MiB per open connection. **CVE ID : CVE-2022-41717**		
Affected Version(s): From (including) 1.19.0 Up to (excluding) 1.19.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Dec-2022	7.5	On Windows, restricted files can be accessed via os.DirFS and http.Dir. The os.DirFS function and http.Dir type provide access to a tree of files rooted at a given directory. These functions permit access to Windows device files under that root. For example, os.DirFS("C:/tmp").Open ("COM1") opens the COM1 device. Both os.DirFS and http.Dir only provide read-only filesystem access. In addition, on Windows, an os.DirFS for the directory (the root of the current drive) can permit a maliciously crafted path to escape from the drive and access any path on the system. With fix applied, the behavior of os.DirFS("") has changed. Previously, an empty root was treated equivalently to "/", so os.DirFS("").Open("tmp") would open the path "/tmp". This now returns an error.	https://groups.google.com/g/golang-announce/c/L_3rmdT0BMU/m/yZDrXjIiBQAJ, https://pkg.go.dev/vuln/GO-2022-1143, https://go.dev/cl/455716, https://go.dev/issue/56694	A-GOL-GO-191222/327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41720		
Allocation of Resources Without Limits or Throttling	08-Dec-2022	5.3	An attacker can cause excessive memory growth in a Go server accepting HTTP/2 requests. HTTP/2 server connections contain a cache of HTTP header keys sent by the client. While the total number of entries in this cache is capped, an attacker sending very large keys can cause the server to allocate approximately 64 MiB per open connection. **CVE ID : CVE-2022-41717**	https://pkg.go.dev/vuln/GO-2022-1144, https://go.dev/cl/455717, https://go.dev/issue/56350, https://go.dev/cl/455635	A-GOL-GO-191222/328
Product: http2					
Affected Version(s): * Up to (excluding) 0.4.0					
Allocation of Resources Without Limits or Throttling	08-Dec-2022	5.3	An attacker can cause excessive memory growth in a Go server accepting HTTP/2 requests. HTTP/2 server connections contain a cache of HTTP header keys sent by the client. While the total number of entries in this cache is capped, an attacker sending very large keys can cause the server to allocate approximately 64 MiB per open connection. **CVE ID : CVE-2022-41717**	https://pkg.go.dev/vuln/GO-2022-1144, https://go.dev/cl/455717, https://go.dev/issue/56350, https://go.dev/cl/455635	A-GOL-HTTP-191222/329
Vendor: Google					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: chrome					
Affected Version(s): * Up to (excluding) 108.0.5359.94					
Access of Resource Using Incompatible Type ('Type Confusion')	02-Dec-2022	8.8	Type confusion in V8 in Google Chrome prior to 108.0.5359.94 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2022-4262**	https://chromereleases.googleblog.com/2022/12/stable-channel-update-for-desktop.html, https://crbug.com/1394403	A-GOO-CHRO-191222/330
Product: tensorflow					
Affected Version(s): * Up to (excluding) 2.8.4					
Out-of-bounds Write	06-Dec-2022	9.1	TensorFlow is an open source platform for machine learning. The function MakeGrapplerFunctionItem takes arguments that determine the sizes of inputs and outputs. If the inputs given are greater than or equal to the sizes of the outputs, an out-of-bounds memory read or a crash is triggered. We have patched the issue in GitHub commit a65411a1d69edfb16b25907ffb8f73556ce36bb7. The fix will be included in TensorFlow 2.11.0. We will also cherrypick this commit on TensorFlow 2.8.4, 2.9.3, and 2.10.1. **CVE ID : CVE-2022-41902**	https://github.com/tensorflow/tensorflow/commit/a65411a1d69edfb16b25907ffb8f73556ce36bb7, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-cg88-rpvp-cjv5	A-GOO-TENS-191222/331
Out-of-bounds Read	06-Dec-2022	9.1	TensorFlow is an open source platform for machine learning. The	https://github.com/tensorflow/tensorflo	A-GOO-TENS-191222/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function MakeGrapplerFunctionItem takes arguments that determine the sizes of inputs and outputs. If the inputs given are greater than or equal to the sizes of the outputs, an out-of-bounds memory read or a crash is triggered. We have patched the issue in GitHub commit a65411a1d69edfb16b25907ffb8f73556ce36bb7. The fix will be included in TensorFlow 2.11.0. We will also cherrypick this commit on TensorFlow 2.8.4, 2.9.3, and 2.10.1. **CVE ID : CVE-2022-41910**	w/commit/a65411a1d69edfb16b25907ffb8f73556ce36bb7, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-frqp-wp83-qggv	
Affected Version(s): 2.10.0					
Out-of-bounds Write	06-Dec-2022	9.1	TensorFlow is an open source platform for machine learning. The function MakeGrapplerFunctionItem takes arguments that determine the sizes of inputs and outputs. If the inputs given are greater than or equal to the sizes of the outputs, an out-of-bounds memory read or a crash is triggered. We have patched the issue in GitHub commit a65411a1d69edfb16b25907ffb8f73556ce36bb7. The fix will be included in TensorFlow 2.11.0. We will also cherrypick this	https://github.com/tensorflow/tensorflow/commit/a65411a1d69edfb16b25907ffb8f73556ce36bb7, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-cg88-rpvp-cjv5	A-GOO-TENS-191222/333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commit on TensorFlow 2.8.4, 2.9.3, and 2.10.1. **CVE ID : CVE-2022-41902**		
Out-of-bounds Read	06-Dec-2022	9.1	TensorFlow is an open source platform for machine learning. The function MakeGrapplerFunctionItem takes arguments that determine the sizes of inputs and outputs. If the inputs given are greater than or equal to the sizes of the outputs, an out-of-bounds memory read or a crash is triggered. We have patched the issue in GitHub commit a65411a1d69edfb16b25907ffb8f73556ce36bb7. The fix will be included in TensorFlow 2.11.0. We will also cherrypick this commit on TensorFlow 2.8.4, 2.9.3, and 2.10.1. **CVE ID : CVE-2022-41910**	https://github.com/tensorflow/tensorflow/commit/a65411a1d69edfb16b25907ffb8f73556ce36bb7, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-frqp-wp83-qggv	A-GOO-TENS-191222/334
Affected Version(s): From (including) 2.9.0 Up to (excluding) 2.9.3					
Out-of-bounds Write	06-Dec-2022	9.1	TensorFlow is an open source platform for machine learning. The function MakeGrapplerFunctionItem takes arguments that determine the sizes of inputs and outputs. If the inputs given are greater than or equal to the sizes of the outputs, an out-of-bounds memory read or a crash is triggered. We	https://github.com/tensorflow/tensorflow/commit/a65411a1d69edfb16b25907ffb8f73556ce36bb7, https://github.com/tensorflow/tensorflow/security/advisories/GH	A-GOO-TENS-191222/335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have patched the issue in GitHub commit a65411a1d69edfb16b25907ffb8f73556ce36bb7. The fix will be included in TensorFlow 2.11.0. We will also cherrypick this commit on TensorFlow 2.8.4, 2.9.3, and 2.10.1. **CVE ID : CVE-2022-41902**	SA-cg88-rpvp-cjv5	
Out-of-bounds Read	06-Dec-2022	9.1	TensorFlow is an open source platform for machine learning. The function MakeGrapplerFunctionItem takes arguments that determine the sizes of inputs and outputs. If the inputs given are greater than or equal to the sizes of the outputs, an out-of-bounds memory read or a crash is triggered. We have patched the issue in GitHub commit a65411a1d69edfb16b25907ffb8f73556ce36bb7. The fix will be included in TensorFlow 2.11.0. We will also cherrypick this commit on TensorFlow 2.8.4, 2.9.3, and 2.10.1. **CVE ID : CVE-2022-41910**	https://github.com/tensorflow/tensorflow/commit/a65411a1d69edfb16b25907ffb8f73556ce36bb7, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-frqp-wp83-qggv	A-GOO-TENS-191222/336
Vendor: goteleport					
Product: teleport					
Affected Version(s): 3.2.2					
Exposure of Resource	08-Dec-2022	6.5	Teleport v3.2.2, Teleport v3.5.6-rc6, and Teleport v3.6.3-b2 was discovered to contain an information	N/A	A-GOT-TELE-191222/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			leak via the /user/get-role-list web interface. **CVE ID : CVE-2022-38599**		
Affected Version(s): 3.5.6					
Exposure of Resource to Wrong Sphere	08-Dec-2022	6.5	Teleport v3.2.2, Teleport v3.5.6-rc6, and Teleport v3.6.3-b2 was discovered to contain an information leak via the /user/get-role-list web interface. **CVE ID : CVE-2022-38599**	N/A	A-GOT-TELE-191222/338
Affected Version(s): 3.6.3					
Exposure of Resource to Wrong Sphere	08-Dec-2022	6.5	Teleport v3.2.2, Teleport v3.5.6-rc6, and Teleport v3.6.3-b2 was discovered to contain an information leak via the /user/get-role-list web interface. **CVE ID : CVE-2022-38599**	N/A	A-GOT-TELE-191222/339
Vendor: gpac					
Product: gpac					
Affected Version(s): 2.0.0					
Out-of-bounds Write	06-Dec-2022	7.8	GPAC MP4box v2.0.0 was discovered to contain a stack overflow in the smil_parse_time_list parameter at /scenegraph/svg_attributes.c. **CVE ID : CVE-2022-45283**	N/A	A-GPA-GPAC-191222/340
Vendor: hasura					
Product: graphql_engine					
Affected Version(s): 2.12.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	08-Dec-2022	8.8	Hasura GraphQL Engine before 2.15.2 mishandles row-level authorization in the Update Many API for Postgres backends. The fixed versions are 2.10.2, 2.11.3, 2.12.1, 2.13.2, 2.14.1, and 2.15.2. (Versions before 2.10.0 are unaffected.) **CVE ID : CVE-2022-46792**	https://hasura.io/blog/critical-vulnerability-in-hasuras-graphql-engine-v2-10-0/, https://groups.google.com/g/hasura-security-announce/c/kzK-uPAKGUU, https://github.com/hasura/graphql-engine/security/advisories/GHSA-g7mj-g7f4-hgrg	A-HAS-GRAP-191222/341
Affected Version(s): 2.14.0					
Incorrect Permission Assignment for Critical Resource	08-Dec-2022	8.8	Hasura GraphQL Engine before 2.15.2 mishandles row-level authorization in the Update Many API for Postgres backends. The fixed versions are 2.10.2, 2.11.3, 2.12.1, 2.13.2, 2.14.1, and 2.15.2. (Versions before 2.10.0 are unaffected.) **CVE ID : CVE-2022-46792**	https://hasura.io/blog/critical-vulnerability-in-hasuras-graphql-engine-v2-10-0/, https://groups.google.com/g/hasura-security-announce/c/kzK-uPAKGUU, https://github.com/hasura/graphql-engine/security/advisories/GHSA-g7mj-g7f4-hgrg	A-HAS-GRAP-191222/342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 2.10.0 Up to (excluding) 2.10.2					
Incorrect Permission Assignment for Critical Resource	08-Dec-2022	8.8	Hasura GraphQL Engine before 2.15.2 mishandles row-level authorization in the Update Many API for Postgres backends. The fixed versions are 2.10.2, 2.11.3, 2.12.1, 2.13.2, 2.14.1, and 2.15.2. (Versions before 2.10.0 are unaffected.) **CVE ID : CVE-2022-46792**	https://hasura.io/blog/critical-vulnerability-in-hasuras-graphql-engine-v2-10-0/, https://groups.google.com/g/hasura-security-announce/c/kzK-uPAKGUU, https://github.com/hasura/graphql-engine/security/advisories/GHSA-g7mj-g7f4-hgrg	A-HAS-GRAP-191222/343
Affected Version(s): From (including) 2.11.0 Up to (excluding) 2.11.3					
Incorrect Permission Assignment for Critical Resource	08-Dec-2022	8.8	Hasura GraphQL Engine before 2.15.2 mishandles row-level authorization in the Update Many API for Postgres backends. The fixed versions are 2.10.2, 2.11.3, 2.12.1, 2.13.2, 2.14.1, and 2.15.2. (Versions before 2.10.0 are unaffected.) **CVE ID : CVE-2022-46792**	https://hasura.io/blog/critical-vulnerability-in-hasuras-graphql-engine-v2-10-0/, https://groups.google.com/g/hasura-security-announce/c/kzK-uPAKGUU, https://github.com/hasura/graphql-engine/security/advisories	A-HAS-GRAP-191222/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				/GHSA-g7mj-g7f4-hgrg	
Affected Version(s): From (including) 2.13.0 Up to (excluding) 2.13.2					
Incorrect Permission Assignment for Critical Resource	08-Dec-2022	8.8	Hasura GraphQL Engine before 2.15.2 mishandles row-level authorization in the Update Many API for Postgres backends. The fixed versions are 2.10.2, 2.11.3, 2.12.1, 2.13.2, 2.14.1, and 2.15.2. (Versions before 2.10.0 are unaffected.) **CVE ID : CVE-2022-46792**	https://hasura.io/blog/critical-vulnerability-in-hasuras-graphql-engine-v2-10-0/, https://groups.google.com/g/hasura-security-announce/c/kzK-uPAKGUU, https://github.com/hasura/graphql-engine/security/advisories/GHSA-g7mj-g7f4-hgrg	A-HAS-GRAP-191222/345
Affected Version(s): From (including) 2.15.0 Up to (excluding) 2.15.2					
Incorrect Permission Assignment for Critical Resource	08-Dec-2022	8.8	Hasura GraphQL Engine before 2.15.2 mishandles row-level authorization in the Update Many API for Postgres backends. The fixed versions are 2.10.2, 2.11.3, 2.12.1, 2.13.2, 2.14.1, and 2.15.2. (Versions before 2.10.0 are unaffected.) **CVE ID : CVE-2022-46792**	https://hasura.io/blog/critical-vulnerability-in-hasuras-graphql-engine-v2-10-0/, https://groups.google.com/g/hasura-security-announce/c/kzK-uPAKGUU, https://github.com/hasura/graphql-engine/securi	A-HAS-GRAP-191222/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ty/advisories /GHSA-g7mj-g7f4-hgrg	
Vendor: Haxx					
Product: curl					
Affected Version(s): * Up to (excluding) 7.86.0					
Exposure of Resource to Wrong Sphere	05-Dec-2022	9.8	When doing HTTP(S) transfers, libcurl might erroneously use the read callback (`CURLOPT_READFUNCTION`) to ask for data to send, even when the `CURLOPT_POSTFIELDS` option has been set, if the same handle previously was used to issue a `PUT` request which used that callback. This flaw may surprise the application and cause it to misbehave and either send off the wrong data or use memory after free or similar in the subsequent `POST` request. The problem exists in the logic for a reused handle when it is changed from a PUT to a POST. **CVE ID : CVE-2022-32221**	N/A	A-HAX-CURL-191222/347
Affected Version(s): From (including) 7.84.0 Up to (excluding) 7.86.0					
Out-of-bounds Write	05-Dec-2022	6.5	curl can be told to parse a `.netrc` file for credentials. If that file endsin a line with 4095 consecutive non-white space letters and no newline, curlwould first read past the end of the	https://hackerone.com/reports/1721098	A-HAX-CURL-191222/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stack-based buffer, and if the readworks, write a zero byte beyond its boundary.This will in most cases cause a segfault or similar, but circumstances might also cause different outcomes.If a malicious user can provide a custom netrc file to an application or otherwise affect its contents, this flaw could be used as denial-of-service. **CVE ID : CVE-2022-35260**		
Vendor: hcltechsw					
Product: hcl_commerce					
Affected Version(s): From (including) 9.1.8 Up to (including) 9.1.11					
N/A	12-Dec-2022	9.8	HCL Commerce, when using Elasticsearch, can allow a remote attacker to cause a denial of service attack on the site and make administrative changes. **CVE ID : CVE-2022-38656**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0101265	A-HCL-HCL_-191222/349
Product: hcl_launch					
Affected Version(s): From (including) 6.2.7.0 Up to (including) 6.2.7.17					
Insufficiently Protected Credentials	12-Dec-2022	4.9	HCL Launch could allow a user with administrative privileges, including "Manage Security" permissions, the ability to recover a credential previously saved for performing authenticated LDAP searches.	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0101208	A-HCL-HCL_-191222/350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42445		
Affected Version(s): From (including) 7.0.0.0 Up to (including) 7.0.5.12					
Insufficiently Protected Credentials	12-Dec-2022	4.9	HCL Launch could allow a user with administrative privileges, including "Manage Security" permissions, the ability to recover a credential previously saved for performing authenticated LDAP searches. **CVE ID : CVE-2022-42445**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0101208	A-HCL-HCL_-191222/351
Affected Version(s): From (including) 7.1.0.0 Up to (including) 7.1.2.8					
Insufficiently Protected Credentials	12-Dec-2022	4.9	HCL Launch could allow a user with administrative privileges, including "Manage Security" permissions, the ability to recover a credential previously saved for performing authenticated LDAP searches. **CVE ID : CVE-2022-42445**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0101208	A-HCL-HCL_-191222/352
Affected Version(s): From (including) 7.2.0.0 Up to (including) 7.2.3.1					
Insufficiently Protected Credentials	12-Dec-2022	4.9	HCL Launch could allow a user with administrative privileges, including "Manage Security" permissions, the ability to recover a credential previously saved for performing authenticated LDAP searches. **CVE ID : CVE-2022-42445**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0101208	A-HCL-HCL_-191222/353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: hcl_workload_automation					
Affected Version(s): * Up to (including) 9.4.0.7					
N/A	12-Dec-2022	7.1	HCL Workload Automation could allow a local user to overwrite key system files which would cause the system to crash. **CVE ID : CVE-2022-38661**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0100939	A-HCL-HCL_-191222/354
Affected Version(s): From (including) 9.5.0.0 Up to (including) 9.5.0.5					
N/A	12-Dec-2022	7.1	HCL Workload Automation could allow a local user to overwrite key system files which would cause the system to crash. **CVE ID : CVE-2022-38661**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0100939	A-HCL-HCL_-191222/355
Vendor: helloprint					
Product: helloprint					
Affected Version(s): * Up to (excluding) 1.4.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	6.1	The Helloprint WordPress plugin before 1.4.7 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-3908**	N/A	A-HEL-HELL-191222/356
Vendor: Hitachi					
Product: jp1\/automatic_operation					
Affected Version(s): 10-01					
Generation of Error Message Containing	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi	https://www.hitachi.co.jp/Prod/comp/soft1/global/s	A-HIT-JP1\-191222/357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	ecurity/info/vuls/hitachi-sec-2022-140/index.html	
Affected Version(s): 10-02					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/358
Affected Version(s): 10-11					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09,	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**		
Affected Version(s): 10-50					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/360
Affected Version(s): 10-51					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/361
Affected Version(s): 11-50					
Generation of Error	06-Dec-2022	3.3	Generation of Error Message Containing	https://www.hitachi.co.jp/	A-HIT-JP1\-191222/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Message Containing Sensitive Information			Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	
Affected Version(s): 12-60					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/363
Affected Version(s): From (including) 10-00 Up to (including) 10-00-02					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**		
Affected Version(s): From (including) 10-10 Up to (including) 10-10-01					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/365
Affected Version(s): From (including) 10-12 Up to (including) 10-12-05					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/366
Affected Version(s): From (including) 10-13 Up to (including) 10-13-04					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/367
Affected Version(s): From (including) 10-52 Up to (including) 10-52-05					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/368
Affected Version(s): From (including) 10-53 Up to (including) 10-53-03					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-	A-HIT-JP1\-191222/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	140/index.html	
Affected Version(s): From (including) 10-54 Up to (including) 10-54-03					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/370
Affected Version(s): From (including) 11-00 Up to (including) 11-00-05					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01.	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34881		
Affected Version(s): From (including) 11-01 Up to (including) 11-01-03					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/372
Affected Version(s): From (including) 11-02 Up to (including) 11-02-01					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/373
Affected Version(s): From (including) 11-10 Up to (including) 11-10-06					
Generation of Error Message Containing	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi	https://www.hitachi.co.jp/Prod/comp/soft1/global/s	A-HIT-JP1\-191222/374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	ecurity/info/vuls/hitachi-sec-2022-140/index.html	
Affected Version(s): From (including) 11-10 Up to (including) 11-10-07					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/375
Affected Version(s): From (including) 11-11 Up to (including) 11-11-04					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09,	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**		
Affected Version(s): From (including) 11-11 Up to (including) 11-11-05					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/377
Affected Version(s): From (including) 11-12 Up to (including) 11-12-03					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/378
Affected Version(s): From (including) 11-12 Up to (including) 11-12-04					
Generation of Error	06-Dec-2022	3.3	Generation of Error Message Containing	https://www.hitachi.co.jp/	A-HIT-JP1\-191222/379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Message Containing Sensitive Information			Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	
Affected Version(s): From (including) 11-51 Up to (including) 11-51-08					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/380
Affected Version(s): From (including) 12-00 Up to (including) 12-00-01					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**		
Affected Version(s): From (including) 12-01 Up to (including) 12-01-02					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/382
Affected Version(s): From (including) 12-10 Up to (including) 12-10-02					
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/383
Affected Version(s): From (including) 12-50 Up to (including) 12-50-01					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	A-HIT-JP1\-191222/384
Vendor: hope-boot_project					
Product: hope-boot					
Affected Version(s): 1.0.0					
Deserialization of Untrusted Data	07-Dec-2022	9.8	hope-boot 1.0.0 has a deserialization vulnerability that can cause Remote Code Execution (RCE). **CVE ID : CVE-2022-44371**	N/A	A-HOP-HOPE-191222/385
Vendor: house_rental_system_project					
Product: house_rental_system					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Dec-2022	9.8	A vulnerability, which was classified as critical, was found in House Rental System. Affected is an unknown function of the file /view-property.php. The manipulation of the argument property_id leads to sql injection. It is possible to launch the attack remotely. The	N/A	A-HOU-HOUS-191222/386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. VDB-214770 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4274**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Dec-2022	9.8	A vulnerability has been found in House Rental System and classified as critical. Affected by this vulnerability is an unknown functionality of the file search-property.php of the component POST Request Handler. The manipulation of the argument search_property leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-214771. **CVE ID : CVE-2022-4275**	N/A	A-HOU-HOUS-191222/387
Unrestricted Upload of File with Dangerous Type	03-Dec-2022	9.8	A vulnerability was found in House Rental System and classified as critical. Affected by this issue is some unknown functionality of the file tenant-engine.php of the component POST Request Handler. The manipulation of the argument id_photo leads to unrestricted upload.	N/A	A-HOU-HOUS-191222/388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-214772. **CVE ID : CVE-2022-4276**		
Vendor: hpe					
Product: oneview_global_dashboard					
Affected Version(s): * Up to (excluding) 2.7					
URL Redirection to Untrusted Site ('Open Redirect')	12-Dec-2022	6.1	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Hewlett Packard Enterprise HPE OneView Global Dashboard (OVGD). **CVE ID : CVE-2022-37927**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04370en_us	A-HPE-ONEV-191222/389
Vendor: human_resource_management_system_project					
Product: human_resource_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	03-Dec-2022	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Human Resource Management System 1.0. This issue affects some unknown processing of the file /hrm/controller/employee.php of the component Content-Type Handler. The manipulation of the argument pfimg leads to unrestricted upload. The attack may be initiated remotely. The exploit has	N/A	A-HUM-HUMA-191222/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. The identifier VDB-214769 was assigned to this vulnerability. **CVE ID : CVE-2022-4273**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Dec-2022	7.2	A vulnerability was found in SourceCodester Human Resource Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /hrm/employeeadd.php. The manipulation of the argument empid leads to sql injection. 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-214775. **CVE ID : CVE-2022-4278**	N/A	A-HUM-HUMA-191222/391
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Dec-2022	6.1	A vulnerability classified as problematic has been found in SourceCodester Human Resource Management System 1.0. Affected is an unknown function of the file /hrm/employeeview.php. The manipulation of the argument search leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public	N/A	A-HUM-HUMA-191222/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and may be used. The identifier of this vulnerability is VDB-214776. **CVE ID : CVE-2022-4279**		
Vendor: IBM					
Product: business_automation_workflow					
Affected Version(s): 20.0.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-2022	6.1	IBM Business Process Manager 21.0.1 through 21.0.3.1, 20.0.0.1 through 20.0.0.2 19.0.0.1 through 19.0.0.3 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: 65687. **CVE ID : CVE-2022-41735**	https://www.ibm.com/support/pages/node/6845496	A-IBM-BUSI-191222/393
Affected Version(s): 20.0.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-2022	6.1	IBM Business Process Manager 21.0.1 through 21.0.3.1, 20.0.0.1 through 20.0.0.2 19.0.0.1 through 19.0.0.3 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	https://www.ibm.com/support/pages/node/6845496	A-IBM-BUSI-191222/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			within a trusted session. IBM X-Force ID: 65687. **CVE ID : CVE-2022-41735**		
Affected Version(s): 21.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-2022	6.1	IBM Business Process Manager 21.0.1 through 21.0.3.1, 20.0.0.1 through 20.0.0.2 19.0.0.1 through 19.0.0.3 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: 65687. **CVE ID : CVE-2022-41735**	https://www.ibm.com/support/pages/node/6845496	A-IBM-BUSI-191222/395
Affected Version(s): 21.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-2022	6.1	IBM Business Process Manager 21.0.1 through 21.0.3.1, 20.0.0.1 through 20.0.0.2 19.0.0.1 through 19.0.0.3 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: 65687. **CVE ID : CVE-2022-41735**	https://www.ibm.com/support/pages/node/6845496	A-IBM-BUSI-191222/396
Affected Version(s): 22.0.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-2022	6.1	IBM Business Process Manager 21.0.1 through 21.0.3.1, 20.0.0.1 through 20.0.0.2 19.0.0.1 through 19.0.0.3 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: 65687. **CVE ID : CVE-2022-41735**	https://www.ibm.com/support/pages/node/6845496	A-IBM-BUSI-191222/397
Affected Version(s): From (including) 19.0.0.1 Up to (including) 19.0.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-2022	6.1	IBM Business Process Manager 21.0.1 through 21.0.3.1, 20.0.0.1 through 20.0.0.2 19.0.0.1 through 19.0.0.3 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: 65687. **CVE ID : CVE-2022-41735**	https://www.ibm.com/support/pages/node/6845496	A-IBM-BUSI-191222/398
Affected Version(s): From (including) 21.0.1 Up to (including) 21.0.3.1					
Improper Neutralization of Input During Web Page	07-Dec-2022	6.1	IBM Business Process Manager 21.0.1 through 21.0.3.1, 20.0.0.1 through 20.0.0.2 19.0.0.1 through 19.0.0.3 is vulnerable to cross-site scripting. This	https://www.ibm.com/support/pages/node/6845496	A-IBM-BUSI-191222/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
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: 65687. **CVE ID : CVE-2022-41735**		
Product: cics_tx					
Affected Version(s): 11.1					
Improper Restriction of Rendered UI Layers or Frames	12-Dec-2022	6.1	IBM CICS TX 11.1 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 229461. **CVE ID : CVE-2022-34318**	https://www.ibm.com/support/pages/node/6833188, https://www.ibm.com/support/pages/node/6833186, https://exchange.xforce.ibmcloud.com/vulnerabilities/229461	A-IBM-CICS-191222/400
Product: cloud_transformation_advisor					
Affected Version(s): From (including) 2.0.1 Up to (excluding) 3.4.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-2022	5.4	IBM Cloud Transformation Advisor 2.0.1 through 3.3.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality	https://www.ibm.com/support/pages/node/6846257	A-IBM-CLOU-191222/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 237214. **CVE ID : CVE-2022-41299**		
Product: content_navigator					
Affected Version(s): From (including) 3.0.0 Up to (including) 3.0.12					
Improper Restriction of Operations within the Bounds of a Memory Buffer	07-Dec-2022	8.8	IBM Content Navigator 3.0.0, 3.0.1, 3.0.2, 3.0.3, 3.0.4, 3.0.5, 3.0.6, 3.0.7, 3.0.8, 3.0.9, 3.0.10, 3.0.11, and 3.0.12 is vulnerable to missing authorization and could allow an authenticated user to load external plugins and execute code. IBM X-Force ID: 238805. **CVE ID : CVE-2022-43581**	https://www.ibm.com/support/pages/node/6844453, https://exchange.xforce.ibmcloud.com/vulnerabilities/238805	A-IBM-CONT-191222/402
Product: db2					
Affected Version(s): 3.5					
Cross-Site Request Forgery (CSRF)	12-Dec-2022	8.8	IBM Db2U 3.5, 4.0, and 4.5 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 237210. **CVE ID : CVE-2022-41296**	https://www.ibm.com/support/pages/node/6843071, https://exchange.xforce.ibmcloud.com/vulnerabilities/237210	A-IBM-DB2-191222/403
Affected Version(s): 4.0					
Cross-Site Request Forgery (CSRF)	12-Dec-2022	8.8	IBM Db2U 3.5, 4.0, and 4.5 is vulnerable to cross-site request forgery which could	https://www.ibm.com/support/pages/node/6843071,	A-IBM-DB2-191222/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 237210. **CVE ID : CVE-2022-41296**	https://exchange.xforce.ibmcloud.com/vulnerabilities/237210	
Affected Version(s): 4.5					
Cross-Site Request Forgery (CSRF)	12-Dec-2022	8.8	IBM Db2U 3.5, 4.0, and 4.5 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 237210. **CVE ID : CVE-2022-41296**	https://www.ibm.com/support/pages/node/6843071, https://exchange.xforce.ibmcloud.com/vulnerabilities/237210	A-IBM-DB2-191222/405
Product: db2u					
Affected Version(s): 3.5					
Cross-Site Request Forgery (CSRF)	01-Dec-2022	6.5	IBM Db2U 3.5, 4.0, and 4.5 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 237212. **CVE ID : CVE-2022-41297**	https://exchange.xforce.ibmcloud.com/vulnerabilities/237212, https://www.ibm.com/support/pages/node/6843071	A-IBM-DB2U-191222/406
Affected Version(s): 4.0					
Cross-Site Request Forgery (CSRF)	01-Dec-2022	6.5	IBM Db2U 3.5, 4.0, and 4.5 is vulnerable to cross-site request forgery which could allow an attacker to	https://exchange.xforce.ibmcloud.com/vulnerabilities/237212,	A-IBM-DB2U-191222/407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 237212. **CVE ID : CVE-2022-41297**	https://www.ibm.com/support/pages/node/6843071	
Affected Version(s): 4.5					
Cross-Site Request Forgery (CSRF)	01-Dec-2022	6.5	IBM Db2U 3.5, 4.0, and 4.5 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 237212. **CVE ID : CVE-2022-41297**	https://exchange.xforce.ibmcloud.com/vulnerabilities/237212, https://www.ibm.com/support/pages/node/6843071	A-IBM-DB2U-191222/408
Product: db2_on_cloud_pak_for_data					
Affected Version(s): From (including) 3.5 Up to (excluding) 4.6					
Cross-Site Request Forgery (CSRF)	01-Dec-2022	6.5	IBM Db2U 3.5, 4.0, and 4.5 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 237212. **CVE ID : CVE-2022-41297**	https://exchange.xforce.ibmcloud.com/vulnerabilities/237212, https://www.ibm.com/support/pages/node/6843071	A-IBM-DB2_-191222/409
Product: db2_warehouse					
Affected Version(s): 3.5					
Cross-Site Request Forgery (CSRF)	12-Dec-2022	8.8	IBM Db2U 3.5, 4.0, and 4.5 is vulnerable to cross-site request forgery which could	https://www.ibm.com/support/pages/node/6843071,	A-IBM-DB2_-191222/410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 237210. **CVE ID : CVE-2022-41296**	https://exchange.xforce.ibmcloud.com/vulnerabilities/237210	
Affected Version(s): 4.0					
Cross-Site Request Forgery (CSRF)	12-Dec-2022	8.8	IBM Db2U 3.5, 4.0, and 4.5 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 237210. **CVE ID : CVE-2022-41296**	https://www.ibm.com/support/pages/node/6843071, https://exchange.xforce.ibmcloud.com/vulnerabilities/237210	A-IBM-DB2_-191222/411
Affected Version(s): 4.5					
Cross-Site Request Forgery (CSRF)	12-Dec-2022	8.8	IBM Db2U 3.5, 4.0, and 4.5 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 237210. **CVE ID : CVE-2022-41296**	https://www.ibm.com/support/pages/node/6843071, https://exchange.xforce.ibmcloud.com/vulnerabilities/237210	A-IBM-DB2_-191222/412
Product: db2_warehouse_on_cloud_pak_for_data					
Affected Version(s): From (including) 3.5 Up to (excluding) 4.6					
Cross-Site Request Forgery (CSRF)	01-Dec-2022	6.5	IBM Db2U 3.5, 4.0, and 4.5 is vulnerable to cross-site request forgery which could allow an attacker to	https://exchange.xforce.ibmcloud.com/vulnerabilities/237212,	A-IBM-DB2_-191222/413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 237212. **CVE ID : CVE-2022-41297**	https://www.ibm.com/support/pages/node/6843071	
Product: spectrum_scale_container_native_storage_access					
Affected Version(s): From (including) 5.1.0.1 Up to (including) 5.1.4.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Dec-2022	7.8	IBM Spectrum Scale 5.1.0.1 through 5.1.4.1 could allow a local attacker to execute arbitrary commands in the container. IBM X-Force ID: 239437. **CVE ID : CVE-2022-43867**	https://www.ibm.com/support/pages/node/6844771	A-IBM-SPEC-191222/414
Product: sterling_secure_proxy					
Affected Version(s): 6.0.3					
Use of a Broken or Risky Cryptographic Algorithm	06-Dec-2022	7.5	IBM Sterling Secure Proxy 6.0.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 230522. **CVE ID : CVE-2022-34361**	https://www.ibm.com/support/pages/node/6844763	A-IBM-STER-191222/415
Product: websphere_automation_for_ibm_cloud_pak_for_watson_aiops					
Affected Version(s): * Up to (excluding) 1.4.3					
Improper Authentication	01-Dec-2022	6.5	IBM WebSphere Automation for IBM Cloud Pak for Watson AIOps 1.4.2 could provide a weaker than	https://www.ibm.com/support/pages/node/6842605, https://excha	A-IBM-WEBS-191222/416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			expected security. A local attacker can create an outbound network connection to another system. IBM X-Force ID: 240827. **CVE ID : CVE-2022-43900**	nge.xforce.ibmcloud.com/vulnerabilities/240827	
Exposure of Resource to Wrong Sphere	01-Dec-2022	5.5	IBM WebSphere Automation for IBM Cloud Pak for Watson AIOps 1.4.3 could disclose sensitive information. An authenticated local attacker could exploit this vulnerability to possibly gain information to other IBM WebSphere Automation for IBM Cloud Pak for Watson AIOps components. IBM X-Force ID: 240829. **CVE ID : CVE-2022-43901**	https://www.ibm.com/support/pages/node/6842605, https://exchange.xforce.ibmcloud.com/vulnerabilities/240829	A-IBM-WEBS-191222/417
Vendor: icegram					
Product: email_subscribers_\&_newsletters					
Affected Version(s): * Up to (excluding) 5.5.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Dec-2022	8.8	The Icegram Express WordPress plugin before 5.5.1 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by any authenticated users, such as subscriber **CVE ID : CVE-2022-3981**	N/A	A-ICE-EMAI-191222/418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Ilias					
Product: ilias					
Affected Version(s): * Up to (excluding) 7.16					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Dec-2022	8.8	ILIAS before 7.16 allows OS Command Injection. **CVE ID : CVE-2022-45915**	N/A	A-ILI-ILIA-191222/419
Externally Controlled Reference to a Resource in Another Sphere	07-Dec-2022	6.5	ILIAS before 7.16 allows External Control of File Name or Path. **CVE ID : CVE-2022-45918**	N/A	A-ILI-ILIA-191222/420
URL Redirection to Untrusted Site ('Open Redirect')	07-Dec-2022	6.1	ILIAS before 7.16 has an Open Redirect. **CVE ID : CVE-2022-45917**	N/A	A-ILI-ILIA-191222/421
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-2022	5.4	ILIAS before 7.16 allows XSS. **CVE ID : CVE-2022-45916**	N/A	A-ILI-ILIA-191222/422
Vendor: inksplat					
Product: comic_book_management_system					
Affected Version(s): * Up to (excluding) 2.2.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Dec-2022	7.2	The Comic Book Management System WordPress plugin before 2.2.0 does not sanitize and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as Admin. **CVE ID : CVE-2022-3856**	N/A	A-INK-COMI-191222/423
Vendor: Interspire					
Product: email_marketer					
Affected Version(s): * Up to (including) 6.5.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Dec-2022	7.5	Interspire Email Marketer through 6.5.1 allows SQL Injection via the surveys module. An unauthenticated attacker could successfully perform an attack to extract potentially sensitive information from the database if the survey id exists. **CVE ID : CVE-2022-44790**	https://www.interspire.com/security-bulletin-2022-44790/	A-INT-EMAI-191222/424
Vendor: isic.lk_project					
Product: isic.lk					
Affected Version(s): * Up to (including) 2018-02-13					
Improper Neutralization of Special Elements used in an SQL Command	01-Dec-2022	9.8	SQL Injection vulnerability in asith-eranga ISIC tour booking through version published on Feb 13th 2018, allows attackers to execute arbitrary commands via the username parameter to /system/user/modules/	N/A	A-ISI-ISIC-191222/425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			mod_users/controller.php. **CVE ID : CVE-2022-30528**		
N/A	01-Dec-2022	7.5	An issue was discovered in asith-eranga ISIC tour booking through version published on Feb 13th 2018, allows attackers to gain sensitive information via the action parameter to /system/user/modules/mod_users/controller.php. **CVE ID : CVE-2022-28607**	N/A	A-ISI-ISIC-191222/426
Vendor: ivanti					
Product: connect_secure					
Affected Version(s): * Up to (excluding) 9.1					
Uncontrolled Resource Consumption	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35254**	N/A	A-IVA-CONN-191222/427
Incorrect Calculation	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure	N/A	A-IVA-CONN-191222/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35258**		
Affected Version(s): 21.12					
Uncontrolled Resource Consumption	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35254**	N/A	A-IVA-CONN-191222/429
Incorrect Calculation	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1.	N/A	A-IVA-CONN-191222/430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35258		
Affected Version(s): 21.9					
Uncontrolled Resource Consumption	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35254**	N/A	A-IVA-CONN-191222/431
Incorrect Calculation	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35258**	N/A	A-IVA-CONN-191222/432
Affected Version(s): 22.1					
Uncontrolled Resource Consumption	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to	N/A	A-IVA-CONN-191222/433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35254**		
Incorrect Calculation	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35258**	N/A	A-IVA-CONN-191222/434
Affected Version(s): 22.2					
Uncontrolled Resource Consumption	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1.	N/A	A-IVA-CONN-191222/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35254		
Incorrect Calculation	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35258**	N/A	A-IVA-CONN-191222/436
Affected Version(s): 9.1					
Uncontrolled Resource Consumption	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35254**	N/A	A-IVA-CONN-191222/437
Incorrect Calculation	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2,	N/A	A-IVA-CONN-191222/438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35258**		
Product: endpoint_manager					
Affected Version(s): * Up to (excluding) 2021.1					
Improper Privilege Management	05-Dec-2022	9.8	A privilege escalation vulnerability is identified in Ivanti EPM (LANDesk Management Suite) that allows a user to execute commands with elevated privileges. **CVE ID : CVE-2022-27773**	https://forums.ivanti.com/s/article/Security-Advisory-for-Ivanti-Endpoint-Manager-Client-CVE-2022-27773?language=en_US	A-IVA-ENDP-191222/439
Affected Version(s): * Up to (including) 2022.3					
XML Injection (aka Blind XPath Injection)	05-Dec-2022	7.8	XML Injection with Endpoint Manager 2022.3 and below causing a download of a malicious file to run and possibly execute to gain unauthorized privileges. **CVE ID : CVE-2022-35259**	https://forums.ivanti.com/s/article/Security-Advisory-for-Ivanti-Endpoint-Manager-Client-CVE-2022-35259?language=en_US	A-IVA-ENDP-191222/440
Affected Version(s): 2021.1					
Improper Privilege Management	05-Dec-2022	9.8	A privilege escalation vulnerability is identified in Ivanti EPM (LANDesk Management Suite) that allows a user to execute	https://forums.ivanti.com/s/article/Security-Advisory-for-Ivanti-Endpoint-	A-IVA-ENDP-191222/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands with elevated privileges. **CVE ID : CVE-2022-27773**	Manager-Client-CVE-2022-27773?language=en_US	
Affected Version(s): 2022					
Improper Privilege Management	05-Dec-2022	9.8	A privilege escalation vulnerability is identified in Ivanti EPM (LANDesk Management Suite) that allows a user to execute commands with elevated privileges. **CVE ID : CVE-2022-27773**	https://forums.ivanti.com/s/article/Security-Advisory-for-Ivanti-Endpoint-Manager-Client-CVE-2022-27773?language=en_US	A-IVA-ENDP-191222/442
Product: neurons_for_zero-trust_access					
Affected Version(s): 22.2					
Uncontrolled Resource Consumption	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35254**	N/A	A-IVA-NEUR-191222/443
Incorrect Calculation	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2,	N/A	A-IVA-NEUR-191222/444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35258**		
Product: policy_secure					
Affected Version(s): * Up to (excluding) 9.1					
Uncontrolled Resource Consumption	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35254**	N/A	A-IVA-POLI-191222/445
Incorrect Calculation	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1.	N/A	A-IVA-POLI-191222/446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35258		
Affected Version(s): 22.1					
Uncontrolled Resource Consumption	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35254**	N/A	A-IVA-POLI-191222/447
Incorrect Calculation	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35258**	N/A	A-IVA-POLI-191222/448
Affected Version(s): 22.2					
Uncontrolled Resource Consumption	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to	N/A	A-IVA-POLI-191222/449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35254**		
Incorrect Calculation	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35258**	N/A	A-IVA-POLI-191222/450
Affected Version(s): 9.1					
Uncontrolled Resource Consumption	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1.	N/A	A-IVA-POLI-191222/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35254		
Incorrect Calculation	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35258**	N/A	A-IVA-POLI-191222/452
Vendor: ixpdata					
Product: easyinstall					
Affected Version(s): 6.6.14725					
Cleartext Storage of Sensitive Information	01-Dec-2022	8.8	IXPdata EasyInstall 6.6.14725 contains an access control issue. **CVE ID : CVE-2022-35120**	N/A	A-IXP-EASY-191222/453
Vendor: Jenkins					
Product: checkmarx					
Affected Version(s): * Up to (excluding) 2022.4.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	5.4	Jenkins Checkmarx Plugin 2022.3.3 and earlier does not escape values returned from the Checkmarx service API before inserting them into HTML reports, resulting in a stored cross-site scripting (XSS) vulnerability.	https://www.jenkins.io/security/advisory/2022-12-07/#SECURITY-2869	A-JEN-CHEC-191222/454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46684		
Product: custom_build_properties					
Affected Version(s): * Up to (including) 2.79.vc095ccc85094					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	5.4	Jenkins Custom Build Properties Plugin 2.79.vc095ccc85094 and earlier does not escape property values and build display names on the Custom Build Properties and Build Summary pages, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to set or change these values. **CVE ID : CVE-2022-46686**	https://www.jenkins.io/security/advisory/2022-12-07/#SECURITY-2810	A-JEN-CUST-191222/455
Product: google_login					
Affected Version(s): From (including) 1.4 Up to (excluding) 1.7					
URL Redirection to Untrusted Site ('Open Redirect')	12-Dec-2022	6.1	Jenkins Google Login Plugin 1.4 through 1.6 (both inclusive) improperly determines that a redirect URL after login is legitimately pointing to Jenkins. **CVE ID : CVE-2022-46683**	https://www.jenkins.io/security/advisory/2022-12-07/#SECURITY-2967	A-JEN-GOOG-191222/456
Product: plot					
Affected Version(s): * Up to (excluding) 2.1.12					
Improper Restriction of XML External Entity Reference	12-Dec-2022	9.8	Jenkins Plot Plugin 2.1.11 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2022-46682**	https://www.jenkins.io/security/advisory/2022-12-07/#SECURITY-2940	A-JEN-PLOT-191222/457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sonar_gerrit					
Affected Version(s): * Up to (including) 377.v8f3808963dc5					
Cross-Site Request Forgery (CSRF)	12-Dec-2022	6.5	A cross-site request forgery (CSRF) vulnerability in Jenkins Sonar Gerrit Plugin 377.v8f3808963dc5 and earlier allows attackers to have Jenkins connect to Gerrit servers (previously configured by Jenkins administrators) using attacker-specified credentials IDs obtained through another method, potentially capturing credentials stored in Jenkins. **CVE ID : CVE-2022-46688**	https://www.jenkins.io/security/advisory/2022-12-07/#SECURITY-1002	A-JEN-SONA-191222/458
Product: spring_config					
Affected Version(s): * Up to (excluding) 2.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	5.4	Jenkins Spring Config Plugin 2.0.0 and earlier does not escape build display names shown on the Spring Config view, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to change build display names. **CVE ID : CVE-2022-46687**	https://www.jenkins.io/security/advisory/2022-12-07/#SECURITY-2814	A-JEN-SPRI-191222/459
Vendor: Jetbrains					
Product: intellij_idea					
Affected Version(s): * Up to (excluding) 2022.2.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-2022	7.8	In JetBrains IntelliJ IDEA before 2022.2.4 a buffer overflow in the fsnotifier daemon on macOS was possible. **CVE ID : CVE-2022-46824**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-INTE-191222/460
Affected Version(s): * Up to (excluding) 2022.3					
Unrestricted Upload of File with Dangerous Type	08-Dec-2022	7.8	In JetBrains IntelliJ IDEA before 2022.3 a DYLIB injection on macOS was possible. **CVE ID : CVE-2022-46828**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-INTE-191222/461
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Dec-2022	5.5	In JetBrains IntelliJ IDEA before 2022.3 the built-in web server allowed an arbitrary file to be read by exploiting a path traversal vulnerability. **CVE ID : CVE-2022-46826**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-INTE-191222/462
Improper Restriction of XML External Entity Reference	08-Dec-2022	5.5	In JetBrains IntelliJ IDEA before 2022.3 an XXE attack leading to SSRF via requests to custom plugin repositories was possible. **CVE ID : CVE-2022-46827**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-INTE-191222/463
Inadequate Encryption Strength	08-Dec-2022	3.3	In JetBrains IntelliJ IDEA before 2022.3 the built-in web server leaked information about open projects. **CVE ID : CVE-2022-46825**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-INTE-191222/464
Product: jetbrains_gateway					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2022.3					
Improper Authentication	08-Dec-2022	8.8	In JetBrains JetBrains Gateway before 2022.3 a client could connect without a valid token if the host consented. **CVE ID : CVE-2022-46829**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-JETB-191222/465
Product: teamcity					
Affected Version(s): From (including) 2022.10 Up to (including) 2022.10.1					
Server-Side Request Forgery (SSRF)	08-Dec-2022	5.3	In JetBrains TeamCity between 2022.10 and 2022.10.1 a custom STS endpoint allowed internal port scanning. **CVE ID : CVE-2022-46830**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-191222/466
Insecure Default Initialization of Resource	08-Dec-2022	4.9	In JetBrains TeamCity between 2022.10 and 2022.10.1 connecting to AWS using the "Default Credential Provider Chain" allowed TeamCity project administrators to access AWS resources normally limited to TeamCity system administrators. **CVE ID : CVE-2022-46831**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-191222/467
Vendor: joinmastodon					
Product: mastodon					
Affected Version(s): * Up to (including) 4.0.2					
Uncontrolled Recursion	04-Dec-2022	7.5	Mastodon through 4.0.2 allows attackers to cause a denial of service (large Sidekiq pull queue) by creating bot accounts that follow attacker-controlled accounts on	N/A	A-JOI-MAST-191222/468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			certain other servers associated with a wildcard DNS A record, such that there is uncontrolled recursion of attacker-generated messages. **CVE ID : CVE-2022-46405**		
Vendor: jrecms					
Product: springbootcms					
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Dec-2022	7.2	A vulnerability was found in SpringBootCMS and classified as critical. Affected by this issue is some unknown functionality of the component Template Management. The manipulation leads to injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-214790 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4282**	N/A	A-JRE-SPRI-191222/469
Vendor: kakaocorp					
Product: potplayer					
Affected Version(s): -					
Improper Resource Shutdown or Release	01-Dec-2022	7.5	A vulnerability classified as problematic has been found in Kakao PotPlayer. This affects an unknown part of the component MID File Handler. The	N/A	A-KAK-POTP-191222/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation leads to denial of service. 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-214623. **CVE ID : CVE-2022-4246**		
Vendor: kbase_doc_project					
Product: kbase_doc					
Affected Version(s): 1.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Dec-2022	9.1	Kbase Doc v1.0 was discovered to contain an arbitrary file deletion vulnerability via the component /web/IndexController.java. **CVE ID : CVE-2022-45290**	N/A	A-KBA-KBAS-191222/471
Vendor: Kibokolabs					
Product: chained_quiz					
Affected Version(s): * Up to (including) 1.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	6.1	The Chained Quiz plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'datef' parameter on the 'chainedquiz_list' page in versions up to, and including, 1.3.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2824193%40chained-quiz&new=2824193%40chained-quiz&sfp_ema	A-KIB-CHAI-191222/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2022-4208**	il=&sfph_mail=	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	6.1	The Chained Quiz plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'pointsf' parameter on the 'chainedquiz_list' page in versions up to, and including, 1.3.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2022-4209**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2824193%40chained-quiz&new=2824193%40chained-quiz&sfp_email=&sfph_mail=	A-KIB-CHAI-191222/473
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	6.1	The Chained Quiz plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'dnf' parameter on the 'chainedquiz_list' page in versions up to, and including, 1.3.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2824193%40chained-quiz&new=2824193%40chained-quiz&sfp_ema	A-KIB-CHAI-191222/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2022-4210**	il=&sfph_mail=	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	6.1	The Chained Quiz plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'emailf' parameter on the 'chainedquiz_list' page in versions up to, and including, 1.3.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2022-4211**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2824193%40chained-quiz&new=2824193%40chained-quiz&sfp_email=&sfph_mail=	A-KIB-CHAI-191222/475
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	6.1	The Chained Quiz plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'ipf' parameter on the 'chainedquiz_list' page in versions up to, and including, 1.3.2 due to insufficient input sanitization and output escaping. This makes it possible for	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2824193%40chained-quiz&new=2824193%40chained-	A-KIB-CHAI-191222/476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2022-4212**	quiz&sfp_email=&sfph_mail=	
Affected Version(s): * Up to (including) 1.3.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	6.1	The Chained Quiz plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'dn' parameter on the 'chainedquiz_list' page in versions up to, and including, 1.3.2.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2022-4213**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2825368%40chained-quiz&new=2825368%40chained-quiz&sfp_email=&sfph_mail=	A-KIB-CHAI-191222/477
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	4.8	The Chained Quiz plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'facebook_appid' parameter in versions up to, and including, 1.3.2.2 due to insufficient input sanitization and output	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2825368%40chained-	A-KIB-CHAI-191222/478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escaping. This makes it possible for authenticated attackers with administrative privileges to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2022-4216**	quiz&new=2825368%40chained-quiz&sfp_email=&sfph_mail=	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	4.8	The Chained Quiz plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'api_key' parameter in versions up to, and including, 1.3.2.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with administrative privileges to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2022-4217**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2825368%40chained-quiz&new=2825368%40chained-quiz&sfp_email=&sfph_mail=, https://plugins.trac.wordpress.org/changeset/2824193	A-KIB-CHAI-191222/479
Affected Version(s): * Up to (including) 1.3.2.3					
Improper Neutralization of Input During Web Page Generation	02-Dec-2022	6.1	The Chained Quiz plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'ip' parameter on the 'chainedquiz_list' page in versions up to, and including, 1.3.2.3 due to	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2826500%40chained	A-KIB-CHAI-191222/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2022-4214**	-quiz&new=2826500%40chained-quiz&sfp_email=&sfph_mail=	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	6.1	The Chained Quiz plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'date' parameter on the 'chainedquiz_list' page in versions up to, and including, 1.3.2.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2022-4215**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2826500%40chained-quiz&new=2826500%40chained-quiz&sfp_email=&sfph_mail=	A-KIB-CHAI-191222/481
Affected Version(s): * Up to (including) 1.3.2.4					
Cross-Site Request Forgery (CSRF)	02-Dec-2022	4.3	The Chained Quiz plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=	A-KIB-CHAI-191222/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including, 1.3.2.4. This is due to missing nonce validation on the list_quizzes() function. This makes it possible for unauthenticated attackers to delete quizzes and copy quizzes via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2022-4218**	&reponame=&old=2826623%40chained-quiz&new=2826623%40chained-quiz&sfp_email=&sfph_mail=	
Cross-Site Request Forgery (CSRF)	02-Dec-2022	4.3	The Chained Quiz plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.3.2.4. This is due to missing nonce validation on the manage() function. This makes it possible for unauthenticated attackers to delete submitted quiz responses via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2022-4219**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2826623%40chained-quiz&new=2826623%40chained-quiz&sfp_email=&sfph_mail=	A-KIB-CHAI-191222/483
Cross-Site Request Forgery (CSRF)	02-Dec-2022	4.3	The Chained Quiz plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.3.2.4. This is due to missing nonce	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=282662	A-KIB-CHAI-191222/484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation on the list_questions() function. This makes it possible for unauthenticated attackers to delete questions from quizzes via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2022-4220**	3%40chained-quiz&new=2826623%40chained-quiz&sfp_email=&sfph_mail=, https://plugins.trac.wordpress.org/browser/chained-quiz/trunk/controllers/questions.php#L73	
Vendor: kodcloud					
Product: kodexplorer					
Affected Version(s): * Up to (excluding) 4.50					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Dec-2022	7.5	Kodexplorer is a chinese language web based file manager and browser based code editor. Versions prior to 4.50 did not prevent unauthenticated users from requesting arbitrary files from the host OS file system. As a result any files available to the host process may be accessed by arbitrary users. This issue has been addressed in version 4.50. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-46154**	https://github.com/kalcaddle/KodExplorer/commit/1f7072c0e12150686f10ee8cda82c004f04be98c	A-KOD-KODE-191222/485
Vendor: kujirahand					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nadesiko3					
Affected Version(s): * Up to (including) 3.3.68					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Dec-2022	9.8	OS command injection vulnerability in Nadesiko3 (PC Version) v3.3.61 and earlier allows a remote attacker to execute an arbitrary OS command when processing compression and decompression on the product. **CVE ID : CVE-2022-41642**	https://github.com/kujirahand/nadesiko3/issues/1325, https://github.com/kujirahand/nadesiko3/issues/1347	A-KUJ-NADE-191222/486
Vendor: Kwoksys					
Product: information_server					
Affected Version(s): * Up to (excluding) 2.9.5					
Improper Restriction of XML External Entity Reference	06-Dec-2022	4.9	An XML external entity (XXE) injection vulnerability in Kwoksys Kwok Information Server before v2.9.5.SP31 allows remote authenticated users to conduct server-side request forgery (SSRF) attacks. **CVE ID : CVE-2022-45326**	https://www.navsec.net/2022/11/12/kwoksys-xxe.html, http://www.kwoksys.com/wiki/index.php?title=Release_Notes	A-KWO-INFO-191222/487
Affected Version(s): 2.9.5					
Improper Restriction of XML External Entity Reference	06-Dec-2022	4.9	An XML external entity (XXE) injection vulnerability in Kwoksys Kwok Information Server before v2.9.5.SP31 allows remote authenticated users to conduct server-side request forgery (SSRF) attacks.	https://www.navsec.net/2022/11/12/kwoksys-xxe.html, http://www.kwoksys.com/wiki/index.php?title=Release_Notes	A-KWO-INFO-191222/488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45326		
Vendor: lazy_mouse_project					
Product: lazy_mouse					
Affected Version(s): * Up to (including) 2.0.1					
Weak Password Requirements	02-Dec-2022	9.8	Lazy Mouse server enforces weak password requirements and doesn't implement rate limiting, allowing remote unauthenticated users to easily and quickly brute force the PIN and execute arbitrary commands. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H **CVE ID : CVE-2022-45482**	N/A	A-LAZ-LAZY-191222/489
Cleartext Transmission of Sensitive Information	02-Dec-2022	5.9	Lazy Mouse allows an attacker (in a man in the middle position between the server and a connected device) to see all data (including keypresses) in cleartext. CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N **CVE ID : CVE-2022-45483**	N/A	A-LAZ-LAZY-191222/490
Vendor: Linuxfoundation					
Product: containerd					
Affected Version(s): * Up to (excluding) 1.5.16					
Uncontrolled Resource Consumption	07-Dec-2022	6.5	containerd is an open source container runtime. A bug was found in containerd's CRI implementation where a user can exhaust memory on the host. In the CRI stream server, a	https://github.com/containerd/containerd/commit/a05d175400b1145e5e6a735a6710579d181e7fb0	A-LIN-CONT-191222/491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			goroutine is launched to handle terminal resize events if a TTY is requested. If the user's process fails to launch due to, for example, a faulty command, the goroutine will be stuck waiting to send without a receiver, resulting in a memory leak. Kubernetes and crictl can both be configured to use containerd's CRI implementation and the stream server is used for handling container IO. This bug has been fixed in containerd 1.6.12 and 1.5.16. Users should update to these versions to resolve the issue. Users unable to upgrade should ensure that only trusted images and commands are used and that only trusted users have permissions to execute commands in running containers. **CVE ID : CVE-2022-23471**		
Affected Version(s): From (including) 1.6.0 Up to (excluding) 1.6.12					
Uncontrolled Resource Consumption	07-Dec-2022	6.5	containerd is an open source container runtime. A bug was found in containerd's CRI implementation where a user can exhaust memory on the host. In the CRI stream server, a goroutine is launched to handle terminal resize	https://github.com/containerd/containerd/commit/a05d175400b1145e5e6a735a6710579d181e7fb0	A-LIN-CONT-191222/492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			events if a TTY is requested. If the user's process fails to launch due to, for example, a faulty command, the goroutine will be stuck waiting to send without a receiver, resulting in a memory leak. Kubernetes and crictl can both be configured to use containerd's CRI implementation and the stream server is used for handling container IO. This bug has been fixed in containerd 1.6.12 and 1.5.16. Users should update to these versions to resolve the issue. Users unable to upgrade should ensure that only trusted images and commands are used and that only trusted users have permissions to execute commands in running containers. **CVE ID : CVE-2022-23471**		
Product: mirage_firewall					
Affected Version(s): From (including) 0.8.0 Up to (excluding) 0.8.4					
Uncontrolled Resource Consumption	07-Dec-2022	7.5	qubes-mirage-firewall (aka Mirage firewall for QubesOS) 0.8.x through 0.8.3 allows guest OS users to cause a denial of service (CPU consumption and loss of forwarding) via a crafted multicast UDP packet (IP address range of	https://github.com/mirage/qubes-mirage-firewall/issues/166	A-LIN-MIRA-191222/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			224.0.0.0 through 239.255.255.255). **CVE ID : CVE-2022-46770**		
Vendor: livemeshelementor					
Product: addons_for_elementor					
Affected Version(s): * Up to (excluding) 7.2.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	4.8	The Livemesh Addons for Elementor WordPress plugin before 7.2.4 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-2022-3862**	N/A	A-LIV-ADDO-191222/494
Vendor: llhttp					
Product: llhttp					
Affected Version(s): * Up to (excluding) 6.0.10					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	05-Dec-2022	9.8	The llhttp parser in the http module in Node v18.7.0 does not correctly handle header fields that are not terminated with CLRF. This may result in HTTP Request Smuggling. **CVE ID : CVE-2022-35256**	N/A	A-LLH-LLHT-191222/495
Vendor: lzmouse					
Product: lazy_mouse					
Affected Version(s): * Up to (including) 2.0.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	05-Dec-2022	9.8	The default configuration of Lazy Mouse does not require a password, allowing remote unauthenticated users to execute arbitrary code with no prior authorization or authentication. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H **CVE ID : CVE-2022-45481**	https://www.synopsys.com/blogs/software-security/cyrc-advisory-remote-code-execution-vulnerabilities-mouse-keyboard-apps/	A-LZM-LAZY-191222/496
Vendor: m-files					
Product: m-files					
Affected Version(s): * Up to (excluding) 22.8.11691.0					
Improper Privilege Management	09-Dec-2022	4.3	Incorrect Privilege Assignment in M-Files Web (Classic) in M-Files before 22.8.11691.0 allows low privilege user to change some configuration. **CVE ID : CVE-2022-4264**	https://www.m-files.com/about/trust-center/security-advisories/cve-2022-4264/	A-M-F-M-FI-191222/497
Product: m-files_server					
Affected Version(s): * Up to (excluding) 22.5.11436.1					
Improper Privilege Management	02-Dec-2022	2.6	Incorrect privilege assignment issue in M-Files Web in M-Files Web versions before 22.5.11436.1 could have changed permissions accidentally. **CVE ID : CVE-2022-4270**	https://www.m-files.com/about/trust-center/security-advisories/cve-2022-4270/	A-M-F-M-FI-191222/498
Vendor: maku					
Product: maku-boot					
Affected Version(s): From (including) 1.3.0 Up to (including) 2.2.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Dec-2022	7.2	A vulnerability, which was classified as critical, was found in maku-boot up to 2.2.0. This affects the function doExecute of the file AbstractScheduleJob.java of the component Scheduled Task Handler. The manipulation leads to injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 446eb7294332efca2bfd791bc37281cedac0d0ff. It is recommended to apply a patch to fix this issue. The identifier VDB-215013 was assigned to this vulnerability. **CVE ID : CVE-2022-4322**	https://gitee.com/makunet/maku-boot/issues/I5ZUYI, https://gitee.com/makunet/maku-boot/commit/446eb7294332efca2bfd791bc37281cedac0d0ff	A-MAK-MAKU-191222/499
Vendor: markdown_preview_enhanced_project					
Product: markdown_preview_enhanced					
Affected Version(s): 0.19.6					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	9.8	Markdown Preview Enhanced v0.6.5 and v0.19.6 for VSCode and Atom was discovered to contain a command injection vulnerability via the PDF file import function. **CVE ID : CVE-2022-45025**	N/A	A-MAR-MARK-191222/500
Improper Neutralization of Special	07-Dec-2022	9.8	An issue in Markdown Preview Enhanced v0.6.5 and v0.19.6 for VSCode and Atom allows	N/A	A-MAR-MARK-191222/501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			attackers to execute arbitrary commands during the GFM export process. **CVE ID : CVE-2022-45026**		
Affected Version(s): 0.6.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Dec-2022	9.8	Markdown Preview Enhanced v0.6.5 and v0.19.6 for VSCode and Atom was discovered to contain a command injection vulnerability via the PDF file import function. **CVE ID : CVE-2022-45025**	N/A	A-MAR-MARK-191222/502
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Dec-2022	9.8	An issue in Markdown Preview Enhanced v0.6.5 and v0.19.6 for VSCode and Atom allows attackers to execute arbitrary commands during the GFM export process. **CVE ID : CVE-2022-45026**	N/A	A-MAR-MARK-191222/503
Vendor: mehanoid					
Product: flat_pm					
Affected Version(s): * Up to (including) 2.661					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	5.4	The Flat PM WordPress plugin through 2.661 does not sanitize and escapes some parameters, which could allow users with a role as low as Admin to perform Cross-Site Scripting attacks.	N/A	A-MEH-FLAT-191222/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3934		
Vendor: Metinfo					
Product: metinfo					
Affected Version(s): 7.7					
Cross-Site Request Forgery (CSRF)	07-Dec-2022	8.8	A Cross-Site Request Forgery (CSRF) in the Administrator List of MetInfo v7.7 allows attackers to arbitrarily add Super Administrator account. **CVE ID : CVE-2022-44849**	N/A	A-MET-METI-191222/505
Vendor: Microfocus					
Product: operations_bridge					
Affected Version(s): * Up to (excluding) 2022.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-2022	5.4	A potential vulnerability has been identified in Micro Focus Operations Bridge - Containerized. The vulnerability could be exploited by a malicious authenticated OBM (Operations Bridge Manager) user to run Java Scripts in the browser context of another OBM user. Please note: The vulnerability is only applicable if the Operations Bridge Manager capability is deployed. A potential vulnerability has been identified in Micro Focus Operations Bridge Manager (OBM). The vulnerability could be exploited by a malicious	https://marketplace.microfocus.com/itom/content/operations-bridge-manager-obm-2022-05-hotfixes, https://portal.microfocus.com/s/article/KM000012517?language=en_US, https://portal.microfocus.com/s/article/KM000012518?language=en_US	A-MIC-OPER-191222/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated OBM user to run Java Scripts in the browser context of another OBM user. This issue affects: Micro Focus Micro Focus Operations Bridge Manager versions prior to 2022.11. Micro Focus Micro Focus Operations Bridge-Containerized versions prior to 2022.11. **CVE ID : CVE-2022-38754**		
Product: operations_bridge_manager					
Affected Version(s): * Up to (excluding) 2022.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-2022	5.4	A potential vulnerability has been identified in Micro Focus Operations Bridge - Containerized. The vulnerability could be exploited by a malicious authenticated OBM (Operations Bridge Manager) user to run Java Scripts in the browser context of another OBM user. Please note: The vulnerability is only applicable if the Operations Bridge Manager capability is deployed. A potential vulnerability has been identified in Micro Focus Operations Bridge Manager (OBM). The vulnerability could be exploited by a malicious authenticated OBM user to run Java Scripts in the browser context of	https://marketplace.microfocus.com/itom/content/operations-bridge-manager-obm-2022-05-hotfixes, https://portal.microfocus.com/s/article/KM000012517?language=en_US, https://portal.microfocus.com/s/article/KM000012518?language=en_US	A-MIC-OPER-191222/507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			another OBM user. This issue affects: Micro Focus Micro Focus Operations Bridge Manager versions prior to 2022.11. Micro Focus Micro Focus Operations Bridge-Containerized versions prior to 2022.11. **CVE ID : CVE-2022-38754**		
Vendor: Microsoft					
Product: windows_firewall					
Affected Version(s): -					
N/A	05-Dec-2022	9.8	A Firewall Rule which allows all incoming TCP connections to all programs from any source and to all ports is created in Windows Firewall after Zabbix agent installation (MSI) **CVE ID : CVE-2022-43516**	https://support.zabbix.com/browse/ZBX-22002	A-MIC-WIND-191222/508
Vendor: mingsoft					
Product: mcms					
Affected Version(s): * Up to (excluding) 5.2.10					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Dec-2022	9.8	A vulnerability was found in Mingsoft MCMS up to 5.2.9. It has been classified as critical. Affected is an unknown function of the file /cms/category/list. The manipulation of the argument sqlWhere leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public	N/A	A-MIN-MCMS-191222/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and may be used. Upgrading to version 5.2.10 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-215196. **CVE ID : CVE-2022-4375**		
Affected Version(s): 5.2.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-2022	6.1	A vulnerability, which was classified as problematic, was found in Mingsoft MCMS 5.2.8. Affected is an unknown function of the file search.do. The manipulation of the argument content_title 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-215112. **CVE ID : CVE-2022-4350**	N/A	A-MIN-MCMS-191222/510
Vendor: Mobatek					
Product: mobaxterm					
Affected Version(s): * Up to (excluding) 22.2					
Improper Authentication	06-Dec-2022	8.1	An access control issue in MobaXterm before v22.1 allows attackers to make connections to the server via the SSH or SFTP	N/A	A-MOB-MOBA-191222/511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocols without authentication. **CVE ID : CVE-2022-38336**		
Affected Version(s): * Up to (including) 22.2					
Use of Hard-coded Credentials	06-Dec-2022	9.1	When aborting a SFTP connection, MobaXterm before v22.1 sends a hardcoded password to the server. The server treats this as an invalid login attempt which can result in a Denial of Service (DoS) for the user if services like fail2ban are used. **CVE ID : CVE-2022-38337**	N/A	A-MOB-MOBA-191222/512
Vendor: movie_ticket_booking_system_project					
Product: movie_ticket_booking_system					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Dec-2022	9.8	A vulnerability classified as critical was found in Movie Ticket Booking System. This vulnerability affects unknown code of the file booking.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-214624. **CVE ID : CVE-2022-4247**	N/A	A-MOV-MOVI-191222/513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Dec-2022	9.8	A vulnerability, which was classified as critical, has been found in Movie Ticket Booking System. This issue affects some unknown processing of the file editBooking.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-214625 was assigned to this vulnerability. **CVE ID : CVE-2022-4248**	N/A	A-MOV-MOVI-191222/514
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-2022	6.1	A vulnerability, which was classified as problematic, was found in Movie Ticket Booking System. Affected is an unknown function of the component POST Request Handler. The manipulation of the argument ORDER_ID 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. VDB-214626 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4249**	N/A	A-MOV-MOVI-191222/515
Improper Neutralization of	01-Dec-2022	6.1	A vulnerability has been found in Movie Ticket Booking System and	N/A	A-MOV-MOVI-191222/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			classified as problematic. Affected by this vulnerability is an unknown functionality of the file booking.php. The manipulation of the argument id leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-214627. **CVE ID : CVE-2022-4250**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-2022	5.4	A vulnerability was found in Movie Ticket Booking System and classified as problematic. Affected by this issue is some unknown functionality of the file editBooking.php. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-214628. **CVE ID : CVE-2022-4251**	N/A	A-MOV-MOVI-191222/517
Vendor: mxsdoc_project					
Product: mxsdoc					
Affected Version(s): -					
Improper Neutralization of	12-Dec-2022	8.8	A vulnerability was found in RainyGao DocSys. It has been	N/A	A-MXS-MXSD-191222/518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			declared as critical. This vulnerability affects the function getReposAllUsers of the file /DocSystem/Repos/getReposAllUsers.do. The manipulation of the argument searchWord/reposId leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-215278 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4416**		
Vendor: nadesiko3_project					
Product: nadesiko3					
Affected Version(s): * Up to (including) 3.3.74					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Dec-2022	9.8	OS command injection vulnerability in Nako3edit, editor component of nadesiko3 (PC Version) v3.3.74 and earlier allows a remote attacker to obtain appkey of the product and execute an arbitrary OS command on the product. **CVE ID : CVE-2022-42496**	https://github.com/kujirahand/nadesiko3/issues/1325	A-NAD-NADE-191222/519
Improper Handling of Exceptiona	05-Dec-2022	7.5	Improper check or handling of exceptional conditions vulnerability in Nako3edit, editor component of nadesiko3 (PC Version) v3.3.74 and	https://github.com/kujirahand/nadesiko3/issues/1325	A-NAD-NADE-191222/520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			earlier allows a remote attacker to inject an invalid value to decodeURIComponent of nako3edit, which may lead the server to crash. **CVE ID : CVE-2022-41777**		
Vendor: neutrinolabs					
Product: xrdp					
Affected Version(s): * Up to (excluding) 0.9.21					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Dec-2022	9.8	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a buffer over flow in xrdp_login_wnd_create() function. There are no known workarounds for this issue. Users are advised to upgrade. **CVE ID : CVE-2022-23468**	N/A	A-NEU-XRDP-191222/521
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Dec-2022	9.8	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a buffer over flow in audin_send_open() function. There are no known workarounds for this issue. Users are advised to upgrade. **CVE ID : CVE-2022-23477**	N/A	A-NEU-XRDP-191222/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	09-Dec-2022	9.8	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a Out of Bound Write in xrdp_mm_trans_process_drdynvc_channel_open() function. There are no known workarounds for this issue. Users are advised to upgrade. **CVE ID : CVE-2022-23478**	N/A	A-NEU-XRDP-191222/523
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Dec-2022	9.8	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a buffer over flow in xrdp_mm_chan_data_in() function. There are no known workarounds for this issue. Users are advised to upgrade. **CVE ID : CVE-2022-23479**	N/A	A-NEU-XRDP-191222/524
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Dec-2022	9.8	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a buffer over flow in devredir_proc_client_devlist_announce_req() function. There are no known workarounds for	N/A	A-NEU-XRDP-191222/525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this issue. Users are advised to upgrade. **CVE ID : CVE-2022-23480**		
Integer Overflow or Wraparound	09-Dec-2022	9.8	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a Integer Overflow in xrdp_mm_process_rail_update_window_text() function. There are no known workarounds for this issue. Users are advised to upgrade. **CVE ID : CVE-2022-23484**	N/A	A-NEU-XRDP-191222/526
Out-of-bounds Read	09-Dec-2022	9.1	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a Out of Bound Read in xrdp_caps_process_confirm_active() function. There are no known workarounds for this issue. Users are advised to upgrade. **CVE ID : CVE-2022-23481**	N/A	A-NEU-XRDP-191222/527
Out-of-bounds Read	09-Dec-2022	9.1	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21	N/A	A-NEU-XRDP-191222/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a Out of Bound Read in xrdp_sec_process_mcs_data_CS_CORE() function. There are no known workarounds for this issue. Users are advised to upgrade. **CVE ID : CVE-2022-23482**		
Out-of-bounds Read	09-Dec-2022	9.1	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a Out of Bound Read in libxrdp_send_to_channel() function. There are no known workarounds for this issue. Users are advised to upgrade. **CVE ID : CVE-2022-23483**	N/A	A-NEU-XRDP-191222/529
Out-of-bounds Read	09-Dec-2022	9.1	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a Out of Bound Read in xrdp_mm_trans_process_drdynvc_channel_close() function. There are no known workarounds for this issue. Users are advised to upgrade. **CVE ID : CVE-2022-23493**	N/A	A-NEU-XRDP-191222/530
Vendor: Nextcloud					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nextcloud_server					
Affected Version(s): 25.0.0					
Incorrect Authorization	01-Dec-2022	5.3	Nextcloud Server is an open source personal cloud server. Prior to versions 24.0.7 and 25.0.1, disabled download shares still allow download through preview images. Images could be downloaded and previews of documents (first page) can be downloaded without being watermarked. Versions 24.0.7 and 25.0.1 contain a fix for this issue. No known workarounds are available. **CVE ID : CVE-2022-41970**	https://github.com/nextcloud/server/pull/34788	A-NEX-NEXT-191222/531
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.0.10					
Uncontrolled Resource Consumption	01-Dec-2022	5.3	Nextcloud Server is an open source personal cloud server. Prior to versions 23.0.10 and 24.0.5, calendar name lengths are not validated before writing to a database. As a result, an attacker can send unnecessary amounts of data against the database. Version 23.0.10 and 24.0.5 contain patches for the issue. No known workarounds are available. **CVE ID : CVE-2022-41968**	https://github.com/nextcloud/server/pull/33139	A-NEX-NEXT-191222/532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.0.11					
Weak Password Requirements	01-Dec-2022	2.7	Nextcloud Server is an open source personal cloud server. Prior to versions 23.0.11, 24.0.7, and 25.0.0, there is no password length limit when creating a user as an administrator. An administrator can cause a limited DoS attack against their own server. Versions 23.0.11, 24.0.7, and 25.0.0 contain a fix for the issue. As a workaround, don't create user accounts with long passwords. **CVE ID : CVE-2022-41969**	https://github.com/nextcloud/server/pull/34500	A-NEX-NEXT-191222/533
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.5					
Uncontrolled Resource Consumption	01-Dec-2022	5.3	Nextcloud Server is an open source personal cloud server. Prior to versions 23.0.10 and 24.0.5, calendar name lengths are not validated before writing to a database. As a result, an attacker can send unnecessary amounts of data against the database. Version 23.0.10 and 24.0.5 contain patches for the issue. No known workarounds are available. **CVE ID : CVE-2022-41968**	https://github.com/nextcloud/server/pull/33139	A-NEX-NEXT-191222/534
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	01-Dec-2022	5.3	Nextcloud Server is an open source personal cloud server. Prior to versions 24.0.7 and 25.0.1, disabled download shares still allow download through preview images. Images could be downloaded and previews of documents (first page) can be downloaded without being watermarked. Versions 24.0.7 and 25.0.1 contain a fix for this issue. No known workarounds are available. **CVE ID : CVE-2022-41970**	https://github.com/nextcloud/server/pull/34788	A-NEX-NEXT-191222/535
Weak Password Requirements	01-Dec-2022	2.7	Nextcloud Server is an open source personal cloud server. Prior to versions 23.0.11, 24.0.7, and 25.0.0, there is no password length limit when creating a user as an administrator. An administrator can cause a limited DoS attack against their own server. Versions 23.0.11, 24.0.7, and 25.0.0 contain a fix for the issue. As a workaround, don't create user accounts with long passwords. **CVE ID : CVE-2022-41969**	https://github.com/nextcloud/server/pull/34500	A-NEX-NEXT-191222/536
Product: nextcloud_talk					
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.2.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	01-Dec-2022	6.5	Nextcould Talk android is a video and audio conferencing app for Nextcloud. Prior to versions 12.2.8, 13.0.10, 14.0.6, and 15.0.0, guests can continue to receive video streams from a call after being removed from a conversation. An attacker would be able to see videos on a call in a public conversation after being removed from that conversation, provided that they were removed while being in the call. Versions 12.2.8, 13.0.10, 14.0.6, and 15.0.0 contain patches for the issue. No known workarounds are available. **CVE ID : CVE-2022-41971**	N/A	A-NEX-NEXT-191222/537
Affected Version(s): From (including) 13.0.0 Up to (excluding) 13.0.10					
Exposure of Resource to Wrong Sphere	01-Dec-2022	6.5	Nextcould Talk android is a video and audio conferencing app for Nextcloud. Prior to versions 12.2.8, 13.0.10, 14.0.6, and 15.0.0, guests can continue to receive video streams from a call after being removed from a conversation. An attacker would be able to see videos on a call in a public conversation after being removed from that conversation, provided that they were removed while being in the call. Versions 12.2.8, 13.0.10,	N/A	A-NEX-NEXT-191222/538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			14.0.6, and 15.0.0 contain patches for the issue. No known workarounds are available. **CVE ID : CVE-2022-41971**		
Affected Version(s): From (including) 14.0.0 Up to (excluding) 14.0.6					
Exposure of Resource to Wrong Sphere	01-Dec-2022	6.5	Nextcould Talk android is a video and audio conferencing app for Nextcloud. Prior to versions 12.2.8, 13.0.10, 14.0.6, and 15.0.0, guests can continue to receive video streams from a call after being removed from a conversation. An attacker would be able to see videos on a call in a public conversation after being removed from that conversation, provided that they were removed while being in the call. Versions 12.2.8, 13.0.10, 14.0.6, and 15.0.0 contain patches for the issue. No known workarounds are available. **CVE ID : CVE-2022-41971**	N/A	A-NEX-NEXT-191222/539
Vendor: NI					
Product: labview_command_line_interface					
Affected Version(s): * Up to (excluding) 22.3.1					
Incorrect Default Permissions	01-Dec-2022	7.8	Incorrect default permissions in the installation folder for NI LabVIEW Command Line Interface (CLI) may allow an authenticated user to potentially enable	https://www.ni.com/en-us/support/documentation/supplemental/22/privilege-escalation-in-	A-NI-LABV-191222/540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege via local access. **CVE ID : CVE-2022-42718**	ni-labview-cli-.html	
Vendor: nodau_project					
Product: nodau					
Affected Version(s): * Up to (excluding) 0.3.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Dec-2022	9.8	A vulnerability was found in TicklishHoneyBee nodau. It has been rated as critical. Affected by this issue is some unknown functionality of the file src/db.c. The manipulation of the argument value/name leads to sql injection. The name of the patch is 7a7d737a3929f335b9717ddbd31db91151b69ad2. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-215252. **CVE ID : CVE-2022-4399**	https://github.com/TicklishHoneyBee/nodau/commit/7a7d737a3929f335b9717ddbd31db91151b69ad2, https://github.com/TicklishHoneyBee/nodau/pull/26	A-NOD-NODA-191222/541
Vendor: nodebb					
Product: nodebb					
Affected Version(s): * Up to (excluding) 2.6.1					
Improper Initialization	05-Dec-2022	9.8	NodeBB is an open source Node.js based forum software. Due to a plain object with a prototype being used in socket.io message handling a specially crafted payload can be used to impersonate other users and takeover	https://github.com/NodeBB/NodeBB/commit/48d143921753914da45926cca6370a92ed0c46b8, https://github.com/NodeB	A-NOD-NODE-191222/542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accounts. This vulnerability has been patched in version 2.6.1. Users are advised to upgrade. Users unable to upgrade may cherry-pick commit `48d143921753914da45926cca6370a92ed0c46b8` into their codebase to patch the exploit. **CVE ID : CVE-2022-46164**	B/NodeBB/security/advisories/GHSA-rf3g-v8p5-p675	
Vendor: Nodejs					
Product: node.js					
Affected Version(s): 18.12.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Dec-2022	8.1	A OS Command Injection vulnerability exists in Node.js versions <14.21.1, <16.18.1, <18.12.1, <19.0.1 due to an insufficient IsAllowedHost check that can easily be bypassed because IsIPAddress does not properly check if an IP address is invalid before making DBS requests allowing rebinding attacks.The fix for this issue in https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32212 was incomplete and this new CVE is to complete the fix. **CVE ID : CVE-2022-43548**	https://nodejs.org/en/blog/vulnerability/november-2022-security-releases/	A-NOD-NODE-191222/543
Affected Version(s): 19.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Dec-2022	8.1	A OS Command Injection vulnerability exists in Node.js versions <14.21.1, <16.18.1, <18.12.1, <19.0.1 due to an insufficient IsAllowedHost check that can easily be bypassed because IsIPAddress does not properly check if an IP address is invalid before making DBS requests allowing rebinding attacks.The fix for this issue in https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32212 was incomplete and this new CVE is to complete the fix. **CVE ID : CVE-2022-43548**	https://nodejs.org/en/blog/vulnerability/november-2022-security-releases/	A-NOD-NODE-191222/544
Affected Version(s): From (including) 14.0.0 Up to (including) 14.14.0					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	05-Dec-2022	9.8	The llhttp parser in the http module in Node v18.7.0 does not correctly handle header fields that are not terminated with CLRF. This may result in HTTP Request Smuggling. **CVE ID : CVE-2022-35256**	N/A	A-NOD-NODE-191222/545
Improper Neutralization of Special Elements used in an OS	05-Dec-2022	8.1	A OS Command Injection vulnerability exists in Node.js versions <14.21.1, <16.18.1, <18.12.1, <19.0.1 due to an insufficient IsAllowedHost check that	https://nodejs.org/en/blog/vulnerability/november-2022-security-releases/	A-NOD-NODE-191222/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			can easily be bypassed because IsIPAddress does not properly check if an IP address is invalid before making DBS requests allowing rebinding attacks.The fix for this issue in https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32212 was incomplete and this new CVE is to complete the fix. **CVE ID : CVE-2022-43548**		
Affected Version(s): From (including) 14.15.0 Up to (excluding) 14.21.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Dec-2022	8.1	A OS Command Injection vulnerability exists in Node.js versions <14.21.1, <16.18.1, <18.12.1, <19.0.1 due to an insufficient IsAllowedHost check that can easily be bypassed because IsIPAddress does not properly check if an IP address is invalid before making DBS requests allowing rebinding attacks.The fix for this issue in https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32212 was incomplete and this new CVE is to complete the fix. **CVE ID : CVE-2022-43548**	https://nodejs.org/en/blog/vulnerability/november-2022-security-releases/	A-NOD-NODE-191222/547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 14.15.0 Up to (including) 14.20.1					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	05-Dec-2022	9.8	The llhttp parser in the http module in Node v18.7.0 does not correctly handle header fields that are not terminated with CLRF. This may result in HTTP Request Smuggling. **CVE ID : CVE-2022-35256**	N/A	A-NOD-NODE-191222/548
Affected Version(s): From (including) 15.0.0 Up to (including) 15.14.0					
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	05-Dec-2022	9.1	A weak randomness in WebCrypto keygen vulnerability exists in Node.js 18 due to a change with EntropySource() in SecretKeyGenTraits::DoKeyGen() in src/crypto/crypto_keygen.cc. There are two problems with this: 1) It does not check the return value, it assumes EntropySource() always succeeds, but it can (and sometimes will) fail. 2) The random data returned byEntropySource() may not be cryptographically strong and therefore not suitable as keying material. **CVE ID : CVE-2022-35255**	N/A	A-NOD-NODE-191222/549
Affected Version(s): From (including) 16.0.0 Up to (including) 16.12.0					
Inconsistent Interpretation of	05-Dec-2022	9.8	The llhttp parser in the http module in Node v18.7.0 does not correctly handle header	N/A	A-NOD-NODE-191222/550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
HTTP Requests ('HTTP Request Smuggling')			fields that are not terminated with CLRF. This may result in HTTP Request Smuggling. **CVE ID : CVE-2022-35256**		
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	05-Dec-2022	9.1	A weak randomness in WebCrypto keygen vulnerability exists in Node.js 18 due to a change with EntropySource() in SecretKeyGenTraits::DoKeyGen() in src/crypto/crypto_keygen.cc. There are two problems with this: 1) It does not check the return value, it assumes EntropySource() always succeeds, but it can (and sometimes will) fail. 2) The random data returned byEntropySource() may not be cryptographically strong and therefore not suitable as keying material. **CVE ID : CVE-2022-35255**	N/A	A-NOD-NODE-191222/551
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Dec-2022	8.1	A OS Command Injection vulnerability exists in Node.js versions <14.21.1, <16.18.1, <18.12.1, <19.0.1 due to an insufficient IsAllowedHost check that can easily be bypassed because IsIPAddress does not properly check if an IP address is invalid before making DBS	https://nodejs.org/en/blog/vulnerability/november-2022-security-releases/	A-NOD-NODE-191222/552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests allowing rebinding attacks.The fix for this issue in https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32212 was incomplete and this new CVE is to complete the fix. **CVE ID : CVE-2022-43548**		
Affected Version(s): From (including) 16.13.0 Up to (excluding) 16.17.1					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	05-Dec-2022	9.8	The llhttp parser in the http module in Node v18.7.0 does not correctly handle header fields that are not terminated with CLRF. This may result in HTTP Request Smuggling. **CVE ID : CVE-2022-35256**	N/A	A-NOD-NODE-191222/553
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	05-Dec-2022	9.1	A weak randomness in WebCrypto keygen vulnerability exists in Node.js 18 due to a change with EntropySource() in SecretKeyGenTraits::DoKeyGen() in src/crypto/crypto_keygen.cc. There are two problems with this: 1) It does not check the return value, it assumes EntropySource() always succeeds, but it can (and sometimes will) fail. 2) The random data returned byEntropySource() may	N/A	A-NOD-NODE-191222/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not be cryptographically strong and therefore not suitable as keying material. **CVE ID : CVE-2022-35255**		
Affected Version(s): From (including) 16.13.0 Up to (excluding) 16.18.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Dec-2022	8.1	A OS Command Injection vulnerability exists in Node.js versions <14.21.1, <16.18.1, <18.12.1, <19.0.1 due to an insufficient IsAllowedHost check that can easily be bypassed because IsIPAddress does not properly check if an IP address is invalid before making DBS requests allowing rebinding attacks.The fix for this issue in https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32212 was incomplete and this new CVE is to complete the fix. **CVE ID : CVE-2022-43548**	https://nodejs.org/en/blog/vulnerability/november-2022-security-releases/	A-NOD-NODE-191222/555
Affected Version(s): From (including) 18.0.0 Up to (excluding) 18.9.1					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	05-Dec-2022	9.8	The llhttp parser in the http module in Node v18.7.0 does not correctly handle header fields that are not terminated with CLRF. This may result in HTTP Request Smuggling.	N/A	A-NOD-NODE-191222/556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35256		
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	05-Dec-2022	9.1	A weak randomness in WebCrypto keygen vulnerability exists in Node.js 18 due to a change with EntropySource() in SecretKeyGenTraits::DoKeyGen() in src/crypto/crypto_keygen.cc. There are two problems with this: 1) It does not check the return value, it assumes EntropySource() always succeeds, but it can (and sometimes will) fail. 2) The random data returned byEntropySource() may not be cryptographically strong and therefore not suitable as keying material. **CVE ID : CVE-2022-35255**	N/A	A-NOD-NODE-191222/557
Affected Version(s): From (including) 18.0.0 Up to (including) 18.11.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Dec-2022	8.1	A OS Command Injection vulnerability exists in Node.js versions <14.21.1, <16.18.1, <18.12.1, <19.0.1 due to an insufficient IsAllowedHost check that can easily be bypassed because IsIPAddress does not properly check if an IP address is invalid before making DBS requests allowing rebinding attacks.The fix for this issue in	https://nodejs.org/en/blog/vulnerability/november-2022-security-releases/	A-NOD-NODE-191222/558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32212 was incomplete and this new CVE is to complete the fix. **CVE ID : CVE-2022-43548**		
Vendor: nokogiri					
Product: nokogiri					
Affected Version(s): 1.13.8					
NULL Pointer Dereference	08-Dec-2022	7.5	Nokogiri is an open source XML and HTML library for the Ruby programming language. Nokogiri `1.13.8` and `1.13.9` fail to check the return value from `xmlTextReaderExpand` in the method `Nokogiri::XML::Reader#attribute_hash`. This can lead to a null pointer exception when invalid markup is being parsed. For applications using `XML::Reader` to parse untrusted inputs, this may potentially be a vector for a denial of service attack. Users are advised to upgrade to Nokogiri `>= 1.13.10`. Users may be able to search their code for calls to either `XML::Reader#attributes` or `XML::Reader#attribute_hash` to determine if they are affected.	https://github.com/sparklemotion/nokogiri/commit/9fe0761c47c0d4270d1a5220cfd25de080350d50, https://github.com/sparklemotion/nokogiri/commit/85410e38410f670cbbc8c5b00d07b843caee88ce	A-NOK-NOKO-191222/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23476		
Affected Version(s): 1.13.9					
NULL Pointer Dereference	08-Dec-2022	7.5	Nokogiri is an open source XML and HTML library for the Ruby programming language. Nokogiri `1.13.8` and `1.13.9` fail to check the return value from `xmlTextReaderExpand` in the method `Nokogiri::XML::Reader#attribute_hash`. This can lead to a null pointer exception when invalid markup is being parsed. For applications using `XML::Reader` to parse untrusted inputs, this may potentially be a vector for a denial of service attack. Users are advised to upgrade to Nokogiri `>= 1.13.10`. Users may be able to search their code for calls to either `XML::Reader#attributes` or `XML::Reader#attribute_hash` to determine if they are affected. **CVE ID : CVE-2022-23476**	https://github.com/sparklemotion/nokogiri/commit/9fe0761c47c0d4270d1a5220cfd25de080350d50, https://github.com/sparklemotion/nokogiri/commit/854103841 0f670cbbc8c5b00d07b843caee88ce	A-NOK-NOKO-191222/560
Vendor: Nttdata					
Product: terasoluna_global_framework					
Affected Version(s): 1.0.0					
Improper Input Validation	05-Dec-2022	7.8	TERASOLUNA Global Framework 1.0.0 (Public review version) and TERASOLUNA Server	N/A	A-NTT-TERA-191222/561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Framework for Java (Rich) 2.0.0.2 to 2.0.5.1 are vulnerable to a ClassLoader manipulation vulnerability due to using the old version of Spring Framework which contains the vulnerability.The vulnerability is caused by an improper input validation issue in the binding mechanism of Spring MVC. By the application processing a specially crafted file, arbitrary code may be executed with the privileges of the application. **CVE ID : CVE-2022-43484**		
Product: terasoluna_server_framework_for_java_\(rich\)					
Affected Version(s): From (including) 2.0.0.2 Up to (excluding) 2.0.5.1					
Improper Input Validation	05-Dec-2022	7.8	TERASOLUNA Global Framework 1.0.0 (Public review version) and TERASOLUNA Server Framework for Java (Rich) 2.0.0.2 to 2.0.5.1 are vulnerable to a ClassLoader manipulation vulnerability due to using the old version of Spring Framework which contains the vulnerability.The vulnerability is caused by an improper input validation issue in the binding mechanism of	N/A	A-NTT-TERA-191222/562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Spring MVC. By the application processing a specially crafted file, arbitrary code may be executed with the privileges of the application. **CVE ID : CVE-2022-43484**		
Vendor: nuxt					
Product: framework					
Affected Version(s): 3.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository nuxt/framework prior to v3.0.0-rc.13. **CVE ID : CVE-2022-4413**	https://github.com/nuxt/framework/commit/253c8f7ee0c0c580c44dedbe9387646264e90a1e, https://huntr.dev/bounties/70ac720d-c932-4ed3-98b1-dd2cbcb90185	A-NUX-FRAM-191222/563
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	6.1	Cross-site Scripting (XSS) - DOM in GitHub repository nuxt/framework prior to v3.0.0-rc.13. **CVE ID : CVE-2022-4414**	https://huntr.dev/bounties/131a41e5-c936-4c3f-84fc-e0e1f0e090b5, https://github.com/nuxt/framework/commit/19a2cd14929ca9b55720cb81f71687830a9e59a4	A-NUX-FRAM-191222/564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: oceanwp					
Product: sticky_header					
Affected Version(s): * Up to (including) 1.0.8					
Cross-Site Request Forgery (CSRF)	04-Dec-2022	6.5	Cross-Site Request Forgery (CSRF) vulnerability in Oceanwp sticky header plugin <= 1.0.8 on WordPress. **CVE ID : CVE-2022-35730**	N/A	A-OCE-STIC-191222/565
Vendor: Offis					
Product: dcmtk					
Affected Version(s): 3.6.7					
Missing Release of Memory after Effective Lifetime	02-Dec-2022	7.5	DCMTK v3.6.7 was discovered to contain a memory leak via the T_ASC_Association object. **CVE ID : CVE-2022-43272**	https://github.com/songxpu/bug_report/tree/master/DCMTK/memory_leak_in_3.6.7	A-OFF-DCMT-191222/566
Vendor: Omron					
Product: cx-programmer					
Affected Version(s): * Up to (including) 9.77					
Use After Free	07-Dec-2022	7.8	Use-after free vulnerability exists in CX-Programmer v.9.77 and earlier, which may lead to information disclosure and/or arbitrary code execution by having a user to open a specially crafted CXP file. **CVE ID : CVE-2022-43508**	N/A	A-OMR-CX-P-191222/567
Out-of-bounds Write	07-Dec-2022	7.8	Out-of-bounds write vulnerability exists in CX-Programmer v.9.77 and earlier, which may lead to information disclosure	N/A	A-OMR-CX-P-191222/568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and/or arbitrary code execution by having a user to open a specially crafted CXP file. **CVE ID : CVE-2022-43509**		
Out-of-bounds Write	07-Dec-2022	7.8	Stack-based buffer overflow vulnerability exists in CX-Programmer v.9.77 and earlier, which may lead to information disclosure and/or arbitrary code execution by having a user to open a specially crafted CXP file. **CVE ID : CVE-2022-43667**	N/A	A-OMR-CX-P-191222/569
Vendor: online_leave_management_system_project					
Product: online_leave_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	07-Dec-2022	7.2	Online Leave Management System v1.0 was discovered to contain an arbitrary file upload vulnerability at /leave_system/classes/SystemSettings.php?f=update_settings. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-45009**	N/A	A-ONL-ONLI-191222/570
Improper Neutralization of Input During Web Page	07-Dec-2022	4.8	Online Leave Management System v1.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the	N/A	A-ONL-ONLI-191222/571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			component /leave_system/admin/?page=maintenance/department. This vulnerability allows attackers to execute arbitrary web scripts or HTML via crafted payload injected into the Name field under the Create New module. **CVE ID : CVE-2022-45008**		
Vendor: openharmony					
Product: openharmony					
Affected Version(s): From (including) 1.1.0 Up to (including) 1.1.5					
Out-of-bounds Write	08-Dec-2022	3.3	Kernel subsystem within OpenHarmony-v3.1.4 and prior versions in kernel_liteos_a has a kernel stack overflow vulnerability when call SysClockGetres. 4 bytes padding data from kernel stack are copied to user space incorrectly and leaked. **CVE ID : CVE-2022-41802**	N/A	A-OPE-OPEN-191222/572
Affected Version(s): From (including) 3.0 Up to (including) 3.0.6					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-2022	7.8	The appspawn and nwebspawn services within OpenHarmony-v3.1.2 and prior versions were found to be vulnerable to buffer overflow vulnerability due to insufficient input validation. An unprivileged malicious application would be	N/A	A-OPE-OPEN-191222/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to gain code execution within any application installed on the device or cause application crash. **CVE ID : CVE-2022-44455**		
Out-of-bounds Write	08-Dec-2022	3.3	Kernel subsystem within OpenHarmony-v3.1.4 and prior versions in kernel_liteos_a has a kernel stack overflow vulnerability when call SysClockGetres. 4 bytes padding data from kernel stack are copied to user space incorrectly and leaked. **CVE ID : CVE-2022-41802**	N/A	A-OPE-OPEN-191222/574
Affected Version(s): From (including) 3.1 Up to (including) 3.1.2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Dec-2022	7.8	The appspawn and nwebspawn services within OpenHarmony-v3.1.2 and prior versions were found to be vulnerable to buffer overflow vulnerability due to insufficient input validation. An unprivileged malicious application would be able to gain code execution within any application installed on the device or cause application crash. **CVE ID : CVE-2022-44455**	N/A	A-OPE-OPEN-191222/575
Affected Version(s): From (including) 3.1 Up to (including) 3.1.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	08-Dec-2022	5.5	OpenHarmony-v3.1.2 and prior versions had a vulnerability that telephony in communication subsystem sends public events with personal data, but the permission is not set. Malicious apps could listen to public events and obtain information such as mobile numbers and SMS data without permissions. **CVE ID : CVE-2022-45118**	N/A	A-OPE-OPEN-191222/576
Improper Authentication	08-Dec-2022	5.3	OpenHarmony-v3.1.4 and prior versions had an vulnerability. PIN code is transmitted to the peer device in plain text during cross-device authentication, which reduces the difficulty of man-in-the-middle attacks. **CVE ID : CVE-2022-45877**	N/A	A-OPE-OPEN-191222/577
Out-of-bounds Write	08-Dec-2022	3.3	Kernel subsystem within OpenHarmony-v3.1.4 and prior versions in kernel_liteos_a has a kernel stack overflow vulnerability when call SysClockGetres. 4 bytes padding data from kernel stack are copied to user space incorrectly and leaked. **CVE ID : CVE-2022-41802**	N/A	A-OPE-OPEN-191222/578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: openrazer_project					
Product: openrazer					
Affected Version(s): * Up to (excluding) 3.5.1					
Out-of-bounds Read	05-Dec-2022	4.6	OpenRazer is an open source driver and user-space daemon to control Razer device lighting and other features on GNU/Linux. Using a modified USB device an attacker can leak stack addresses of the `razer_attr_read_dpi_stages`, potentially bypassing KASLR. To exploit this vulnerability an attacker would need to access to a users keyboard or mouse or would need to convince a user to use a modified device. The issue has been patched in v3.5.1. Users are advised to upgrade and should be reminded not to plug in unknown USB devices. **CVE ID : CVE-2022-23467**	https://github.com/openrazer/openrazer/security/advisories/GHSA-39hg-jvc9-fg7h, https://github.com/openrazer/openrazer/commit/33aa7f07d54ae066f201c6d298cb4a2181cb90e6	A-OPE-OPEN-191222/579
Vendor: paddlepaddle					
Product: paddlepaddle					
Affected Version(s): * Up to (excluding) 2.4					
Out-of-bounds Read	07-Dec-2022	9.1	Out-of-bounds read in gather_tree in PaddlePaddle before 2.4. **CVE ID : CVE-2022-46741**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2022-001.md	A-PAD-PADD-191222/580
Affected Version(s): 2.4.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	07-Dec-2022	9.8	Code injection in paddle.audio.functional.get_window in PaddlePaddle 2.4.0-rc0 allows arbitrary code execution. **CVE ID : CVE-2022-46742**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2022-002.md	A-PAD-PADD-191222/581
Vendor: pallidlight_online_course_selection_system_project					
Product: pallidlight_online_course_selection_system					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Dec-2022	5.4	A vulnerability was found in pallidlight online-course-selection-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 identifier of this vulnerability is VDB-215268. **CVE ID : CVE-2022-4401**	N/A	A-PAL-PALL-191222/582
Vendor: passeo_project					
Product: passeo					
Affected Version(s): * Up to (excluding) 1.0.5					
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	06-Dec-2022	7.5	Passeo is an open source python password generator. Versions prior to 1.0.5 rely on the python `random` library for random value selection. The python `random` library warns that it should not be used for security purposes due to its reliance on a non-	https://github.com/ArjunSharda/Passeo/commit/8caa798b6bc4647dca59b2376204b6dc6176361a	A-PAS-PASS-191222/583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cryptographically secure random number generator. As a result a motivated attacker may be able to guess generated passwords. This issue has been addressed in version 1.0.5. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2022-23472**		
Vendor: pb-cms_project					
Product: pb-cms					
Affected Version(s): 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-2022	9.6	A vulnerability was found in LinZhaoguan pb-cms 2.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /blog/comment of the component Message Board. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-215114 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4354**	N/A	A-PB--PB-C-191222/584
Improper Neutralization of Input During	08-Dec-2022	9	A vulnerability has been found in LinZhaoguan pb-cms 2.0 and classified as problematic. Affected by this vulnerability is	N/A	A-PB--PB-C-191222/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			the function IpUtil.getIpAddr. 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. The identifier VDB-215113 was assigned to this vulnerability. **CVE ID : CVE-2022-4353**		
Vendor: pdfmake_project					
Product: pdfmake					
Affected Version(s): * Up to (including) 0.2.5					
Improper Control of Generation of Code ('Code Injection')	06-Dec-2022	9.8	pdfmake is an open source client/server side PDF printing in pure JavaScript. In versions up to and including 0.2.5 pdfmake contains an unsafe evaluation of user controlled input. Users of pdfmake are thus subject to arbitrary code execution in the context of the process running the pdfmake code. There are no known fixes for this issue. Users are advised to restrict access to trusted user input. **CVE ID : CVE-2022-46161**	N/A	A-PDF-PDFM-191222/586
Vendor: Phpmyfaq					
Product: phpmyfaq					
Affected Version(s): * Up to (excluding) 3.1.9					
Cleartext Transmission of	11-Dec-2022	7.5	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute in	https://github.com/thorsten/phpmyfaq/	A-PHP-PHPM-191222/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			GitHub repository thorsten/phpmyfaq prior to 3.1.9. **CVE ID : CVE-2022-4409**	commit/8b47f38, https://huntr.dev/bounties/5915ed4c-5fe2-42e7-8fac-5dd0d032727c	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Dec-2022	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository thorsten/phpmyfaq prior to 3.1.9. **CVE ID : CVE-2022-4407**	https://huntr.dev/bounties/a1649f43-78c9-4927-b313-36911872a84b, https://github.com/thorsten/phpmyfaq/commit/1d73af34bf42764f9f9491c7ba5e9495d70e3ca5	A-PHP-PHPM-191222/588
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Dec-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.9. **CVE ID : CVE-2022-4408**	https://huntr.dev/bounties/2ec4ddd4-de22-4f2d-ba92-3382b452bfea, https://github.com/thorsten/phpmyfaq/commit/e2ea332a2b5e798f2c39203b2489a2dabe831751	A-PHP-PHPM-191222/589
Vendor: pinterest					
Product: querybook					
Affected Version(s): * Up to (excluding) 3.14.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	Querybook is an open source data querying UI. In affected versions user provided data is not escaped in the error field of the auth callback url in `querybook/server/app/auth/oauth_auth.py` and `querybook/server/app/auth/okta_auth.py`. This may allow attackers to perform reflected cross site scripting (XSS) if Content Security Policy (CSP) is not enabled or `unsafe-inline` is allowed. Users are advised to upgrade to the latest, patched version of querybook (version 3.14.2 or greater). Users unable to upgrade may enable CSP and not allow unsafe-inline or manually escape query parameters in a reverse proxy. **CVE ID : CVE-2022-46151**	https://github.com/pinterest/querybook/commit/88a7f10495bf5ed1a556ade51a2f2794e403c063	A-PIN-QUER-191222/590
Vendor: podman_project					
Product: podman					
Affected Version(s): 4.1.0					
Relative Path Traversal	08-Dec-2022	3.3	A flaw was found in Buildah. The local path and the lowest subdirectory may be disclosed due to incorrect absolute path traversal, resulting in an impact to confidentiality. **CVE ID : CVE-2022-4123**	N/A	A-POD-PODM-191222/591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 4.1.1					
Relative Path Traversal	08-Dec-2022	3.3	A flaw was found in Buildah. The local path and the lowest subdirectory may be disclosed due to incorrect absolute path traversal, resulting in an impact to confidentiality. **CVE ID : CVE-2022-4123**	N/A	A-POD-PODM-191222/592
Affected Version(s): 4.2.0					
Relative Path Traversal	08-Dec-2022	3.3	A flaw was found in Buildah. The local path and the lowest subdirectory may be disclosed due to incorrect absolute path traversal, resulting in an impact to confidentiality. **CVE ID : CVE-2022-4123**	N/A	A-POD-PODM-191222/593
Affected Version(s): 4.2.1					
Relative Path Traversal	08-Dec-2022	3.3	A flaw was found in Buildah. The local path and the lowest subdirectory may be disclosed due to incorrect absolute path traversal, resulting in an impact to confidentiality. **CVE ID : CVE-2022-4123**	N/A	A-POD-PODM-191222/594
Affected Version(s): 4.3.0					
Improper Link Resolution Before File Access	08-Dec-2022	5.3	A vulnerability was found in buildah. Incorrect following of symlinks while reading .containerignore and	https://github.com/containers/podman/pull/16315	A-POD-PODM-191222/595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Link Following')			.dockerignore results in information disclosure. **CVE ID : CVE-2022-4122**		
Relative Path Traversal	08-Dec-2022	3.3	A flaw was found in Buildah. The local path and the lowest subdirectory may be disclosed due to incorrect absolute path traversal, resulting in an impact to confidentiality. **CVE ID : CVE-2022-4123**	N/A	A-POD-PODM-191222/596
Vendor: postmagthemes					
Product: postmagthemes_demo_import					
Affected Version(s): * Up to (including) 1.0.7					
Unrestricted Upload of File with Dangerous Type	05-Dec-2022	7.2	The PostmagThemes Demo Import WordPress plugin through 1.0.7 does not validate the imported file, allowing high-privilege users such as admin to upload arbitrary files (such as PHP) leading to RCE. **CVE ID : CVE-2022-1540**	N/A	A-POS-POST-191222/597
Vendor: premio					
Product: chaty					
Affected Version(s): * Up to (excluding) 3.0.3					
Improper Neutralization of Special Elements used in an SQL Command	05-Dec-2022	7.2	The Floating Chat Widget: Contact Chat Icons, Telegram Chat, Line, WeChat, Email, SMS, Call Button WordPress plugin before 3.0.3 does not properly sanitise and escape a parameter before using it	N/A	A-PRE-CHAT-191222/598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			in a SQL statement, leading to a SQL injection exploitable by users with a role as low as admin. **CVE ID : CVE-2022-3858**		
Vendor: Prestashop					
Product: prestashop					
Affected Version(s): * Up to (excluding) 1.7.8.8					
Exposure of Sensitive Information to an Unauthorized Actor	08-Dec-2022	4.3	PrestaShop is an open-source e-commerce solution. Versions prior to 1.7.8.8 did not properly restrict host filesystem access for users. Users may have been able to view the contents of the upload directory without appropriate permissions. This issue has been addressed and users are advised to upgrade to version 1.7.8.8. There are no known workarounds for this issue. **CVE ID : CVE-2022-46158**	https://github.com/PrestaShop/PrestaShop/commit/8684d429fb7c3bb51efb098e8b92a1fd2958f8cf	A-PRE-PRES-191222/599
Vendor: Proofpoint					
Product: enterprise_protection					
Affected Version(s): * Up to (including) 8.19.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	9.6	The Admin Smart Search feature in Proofpoint Enterprise Protection (PPS/PoD) contains a stored cross-site scripting vulnerability that enables an anonymous email sender to gain admin privileges within the user interface.	https://www.proofpoint.com/security/security-advisories/pfpt-sa-2022-0002	A-PRO-ENTE-191222/600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This affects all versions 8.19.0 and below. **CVE ID : CVE-2022-46332**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Dec-2022	7.2	The admin user interface in Proofpoint Enterprise Protection (PPS/PoD) contains a command injection vulnerability that enables an admin to execute commands beyond their allowed scope. This affects all versions 8.19.0 and below. **CVE ID : CVE-2022-46333**	https://www.proofpoint.com/security/security-advisories/pfpt-sa-2022-0003	A-PRO-ENTE-191222/601
Vendor: protocol					
Product: go-merkledag					
Affected Version(s): From (including) 0.4.0 Up to (excluding) 0.8.1					
Unchecked Return Value	08-Dec-2022	7.5	go-merkledag implements the 'DAGService' interface and adds two ipld node types, Protobuf and Raw for the ipfs project. A `ProtoNode` may be modified in such a way as to cause various encode errors which will trigger a panic on common method calls that don't allow for error returns. A `ProtoNode` should only be able to encode to valid DAG-PB, attempting to encode invalid DAG-PB forms will result in an error from the codec. Manipulation of an existing (newly created or decoded) `ProtoNode`	https://github.com/ipfs/go-merkledag/pull/93, https://github.com/ipfs/go-merkledag/pull/91, https://github.com/ipfs/kubo/issues/9297, https://github.com/ipfs/go-merkledag/pull/92, https://github.com/ipfs/go-	A-PRO-GO-M-191222/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using the modifier methods did not account for certain states that would place the `ProtoNode` into an unencodeable form. Due to conformance with the [`github.com/ipfs/go-block-format#Block`](https://pkg.go.dev/github.com/ipfs/go-block-format#Block) and [`github.com/ipfs/go-ipld-format#Node`](https://pkg.go.dev/github.com/ipfs/go-ipld-format#Node) interfaces, certain methods, which internally require a re-encode if state has changed, will panic due to the inability to return an error. This issue has been addressed across a number of pull requests. Users are advised to upgrade to version 0.8.1 for a complete set of fixes. Users unable to upgrade may attempt to mitigate this issue by sanitising inputs when allowing user-input to set a new `CidBuilder` on a `ProtoNode` and by sanitising `Tsize` (`Link#Size`) values such that they are a reasonable byte-size for sub-DAGs where derived from user-input.	merkledag/issues/90	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23495		
Product: libp2p					
Affected Version(s): * Up to (excluding) 0.18.0					
Uncontrolled Resource Consumption	08-Dec-2022	7.5	go-libp2p is the offical libp2p implementation in the Go programming language. Version `0.18.0` and older of go-libp2p are vulnerable to targeted resource exhaustion attacks. These attacks target libp2p's connection, stream, peer, and memory management. An attacker can cause the allocation of large amounts of memory, ultimately leading to the process getting killed by the host's operating system. While a connection manager tasked with keeping the number of connections within manageable limits has been part of go-libp2p, this component was designed to handle the regular churn of peers, not a targeted resource exhaustion attack. Users are advised to upgrade their version of go-libp2p to version `0.18.1` or newer. Users unable to upgrade may consult the denial of service (dos) mitigation page for more information on how to incorporate mitigation	https://docs.libp2p.io/reference/dos-mitigation/, https://github.com/libp2p/go-libp2p/commit/15d7dfbf54264ead8e6f49ca658d79c90635e2de	A-PRO-LIBP-191222/603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			strategies, monitor your application, and respond to attacks. **CVE ID : CVE-2022-23492**		
Affected Version(s): * Up to (excluding) 0.38.0					
Uncontrolled Resource Consumption	07-Dec-2022	7.5	js-libp2p is the official javascript Implementation of libp2p networking stack. Versions older than `v0.38.0` of js-libp2p are vulnerable to targeted resource exhaustion attacks. These attacks target libp2p's connection, stream, peer, and memory management. An attacker can cause the allocation of large amounts of memory, ultimately leading to the process getting killed by the host's operating system. While a connection manager tasked with keeping the number of connections within manageable limits has been part of js-libp2p, this component was designed to handle the regular churn of peers, not a targeted resource exhaustion attack. Users are advised to update their js-libp2p dependency to `v0.38.0` or greater. There are no known workarounds for this vulnerability.	N/A	A-PRO-LIBP-191222/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23487		
Affected Version(s): * Up to (excluding) 0.45.1					
Uncontrolled Resource Consumption	07-Dec-2022	7.5	libp2p-rust is the official rust language Implementation of the libp2p networking stack. In versions prior to 0.45.1 an attacker node can cause a victim node to allocate a large number of small memory chunks, which can ultimately lead to the victim's process running out of memory and thus getting killed by its operating system. When executed continuously, this can lead to a denial of service attack, especially relevant on a larger scale when run against more than one node of a libp2p based network. Users are advised to upgrade to `libp2p` `v0.45.1` or above. Users unable to upgrade should reference the DoS Mitigation page for more information on how to incorporate mitigation strategies, monitor their application, and respond to attacks: https://docs.libp2p.io/reference/dos-mitigation/. **CVE ID : CVE-2022-23486**	N/A	A-PRO-LIBP-191222/605
Vendor: Proxmox					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: proxmox_mail_gateway					
Affected Version(s): -					
Server-Side Request Forgery (SSRF)	04-Dec-2022	9.8	Proxmox Virtual Environment (PVE) and Proxmox Mail Gateway (PMG) are vulnerable to SSRF when proxying HTTP requests between pve(pmg)proxy and pve(pmg)daemon. An attacker with an unprivileged account can craft an HTTP request to achieve SSRF and file disclosure of any files on the server. Also, in Proxmox Mail Gateway, privilege escalation to the root@pam account is possible if the backup feature has ever been used, because backup files such as pmg-backup_YYYY_MM_DD_*.tgz have 0644 permissions and contain an authkey value. This is fixed in pve-http-server 4.1-3. **CVE ID : CVE-2022-35508**	https://git.proxmox.com/?p=pve-http-server.git;a=commitdiff;h=c2bd69c7b5e9c775f96021cf8ae53da3dbd9029d, https://git.proxmox.com/?p=pve-http-server.git;a=commitdiff;h=580d540ea907ba15f64379c5bb69ecf1a49a875f	A-PRO-PROX-191222/606
Improper Neutralization of Special Elements in Output Used by a Downstream Component	04-Dec-2022	7.1	A response-header CRLF injection vulnerability in the Proxmox Virtual Environment (PVE) and Proxmox Mail Gateway (PMG) web interface allows a remote attacker to set cookies for a victim's browser that are longer than the server expects, causing a client-side DoS. This affects	https://git.proxmox.com/?p=pve-http-server.git;a=commitdiff;h=936007ae024181109315500486da171379c23c2, https://starlabs.sg/blog/2022/12-	A-PRO-PROX-191222/607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')			Chromium-based browsers because they allow injection of response headers with %0d. This is fixed in pve-http-server 4.1-3. **CVE ID : CVE-2022-35507**	multiple-vulnerabilites-in-proxmox-ve--proxmox-mail-gateway/	
Product: pve_http_server					
Affected Version(s): * Up to (excluding) 4.1-3					
Server-Side Request Forgery (SSRF)	04-Dec-2022	9.8	Proxmox Virtual Environment (PVE) and Proxmox Mail Gateway (PMG) are vulnerable to SSRF when proxying HTTP requests between pve(pmg)proxy and pve(pmg)daemon. An attacker with an unprivileged account can craft an HTTP request to achieve SSRF and file disclosure of any files on the server. Also, in Proxmox Mail Gateway, privilege escalation to the root@pam account is possible if the backup feature has ever been used, because backup files such as pmg-backup_YYYY_MM_DD_*.tgz have 0644 permissions and contain an authkey value. This is fixed in pve-http-server 4.1-3. **CVE ID : CVE-2022-35508**	https://git.proxmox.com/?p=pve-http-server.git;a=commitdiff;h=c2bd69c7b5e9c775f96021cf8ae53da3dbd9029d, https://git.proxmox.com/?p=pve-http-server.git;a=commitdiff;h=580d540ea907ba15f64379c5bb69ecf1a49a875f	A-PRO-PVE_-191222/608
Improper Neutralization of	04-Dec-2022	7.1	A response-header CRLF injection vulnerability in the Proxmox Virtual	https://git.proxmox.com/?p=pve-http-	A-PRO-PVE_-191222/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements in Output Used by a Downstream Component ('Injection')			Environment (PVE) and Proxmox Mail Gateway (PMG) web interface allows a remote attacker to set cookies for a victim's browser that are longer than the server expects, causing a client-side DoS. This affects Chromium-based browsers because they allow injection of response headers with %0d. This is fixed in pve-http-server 4.1-3. **CVE ID : CVE-2022-35507**	server.git;a=commitdiff;h=936007ae024181109315500486da171379c23c2, https://starlabs.sg/blog/2022/12-multiple-vulnerabilites-in-proxmox-ve--proxmox-mail-gateway/	
Product: virtual_environment					
Affected Version(s): -					
Server-Side Request Forgery (SSRF)	04-Dec-2022	9.8	Proxmox Virtual Environment (PVE) and Proxmox Mail Gateway (PMG) are vulnerable to SSRF when proxying HTTP requests between pve(pmg)proxy and pve(pmg)daemon. An attacker with an unprivileged account can craft an HTTP request to achieve SSRF and file disclosure of any files on the server. Also, in Proxmox Mail Gateway, privilege escalation to the root@pam account is possible if the backup feature has ever been used, because backup files such as pmg-backup_YYYY_MM_DD_*.tgz have 0644 permissions and contain	https://git.proxmox.com/?p=pve-http-server.git;a=commitdiff;h=c2bd69c7b5e9c775f96021cf8ae53da3dbd9029d, https://git.proxmox.com/?p=pve-http-server.git;a=commitdiff;h=580d540ea907ba15f64379c5bb69ecf1a49a875f	A-PRO-VIRT-191222/610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an authkey value. This is fixed in pve-http-server 4.1-3. **CVE ID : CVE-2022-35508**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Dec-2022	7.1	A response-header CRLF injection vulnerability in the Proxmox Virtual Environment (PVE) and Proxmox Mail Gateway (PMG) web interface allows a remote attacker to set cookies for a victim's browser that are longer than the server expects, causing a client-side DoS. This affects Chromium-based browsers because they allow injection of response headers with %0d. This is fixed in pve-http-server 4.1-3. **CVE ID : CVE-2022-35507**	https://git.proxmox.com/?p=pve-http-server.git;a=commitdiff;h=936007ae024181109315500486da171379c23c2, https://starlabs.sg/blog/2022/12-multiple-vulnerabilites-in-proxmox-ve--proxmox-mail-gateway/	A-PRO-VIRT-191222/611
Vendor: Pulsesecure					
Product: pulse_connect_secure					
Affected Version(s): 9.1					
Uncontrolled Resource Consumption	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-	N/A	A-PUL-PULS-191222/612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35254**		
Incorrect Calculation	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35258**	N/A	A-PUL-PULS-191222/613
Product: pulse_policy_secure					
Affected Version(s): 9.1					
Uncontrolled Resource Consumption	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35254**	N/A	A-PUL-PULS-191222/614
Incorrect Calculation	05-Dec-2022	7.5	An unauthenticated attacker can cause a denial-of-service to the	N/A	A-PUL-PULS-191222/615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			following products: Ivanti Connect Secure (ICS) in versions prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R4, Ivanti Policy Secure (IPS) in versions prior to 9.1R17 and 22.3R1, and Ivanti Neurons for Zero-Trust Access in versions prior to 22.3R1. **CVE ID : CVE-2022-35258**		
Vendor: pwndoc_project					
Product: pwndoc					
Affected Version(s): 0.5.3					
N/A	05-Dec-2022	8.8	An issue in the /api/audits component of Pwndoc v0.5.3 allows attackers to escalate privileges and execute arbitrary code via uploading a crafted audit file. **CVE ID : CVE-2022-45771**	N/A	A-PWN-PWND-191222/616
Vendor: pwn_project					
Product: pwn					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	08-Dec-2022	6.8	A vulnerability classified as problematic has been found in CTF-hacker pwn. This affects an unknown part of the file delete.html. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the	N/A	A-PWN-PWN-191222/617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. The identifier VDB-215109 was assigned to this vulnerability. **CVE ID : CVE-2022-4349**		
Vendor: py7zr_project					
Product: py7zr					
Affected Version(s): * Up to (excluding) 0.20.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Dec-2022	9.1	A directory traversal vulnerability in the SevenZipFile.extractall() function of the python library py7zr v0.20.0 and earlier allows attackers to write arbitrary files via extracting a crafted 7z file. **CVE ID : CVE-2022-44900**	https://github.com/miurahr/py7zr/commit/1bb43f17515c7f69673a1c88ab9cc72a7bbef406	A-PY7-PY7Z-191222/618
Vendor: pyrdfa3_project					
Product: pyrdfa3					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2022	5.4	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in RDFlib pyrdfa3 and classified as problematic. This issue affects the function _get_option of the file pyRdfa/__init__.py. The manipulation leads to cross site scripting. The attack may be initiated remotely. The name of the patch is ffd1d62dd50d5f4190013b39cedcdfbd81f3ce3e. It is recommended to apply a patch to fix this issue.	https://github.com/RDFLib/pyrdfa3/commit/ffd1d62dd50d5f4190013b39cedcdfbd81f3ce3e, https://github.com/RDFLib/pyrdfa3/pull/40	A-PYR-PYRD-191222/619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The identifier VDB-215249 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2022-4396**		
Vendor: quarkus					
Product: quarkus					
Affected Version(s): From (including) 2.0 Up to (excluding) 2.13.5					
N/A	06-Dec-2022	7.5	Quarkus CORS filter allows simple GET and POST requests with invalid Origin to proceed. Simple GET or POST requests made with XMLHttpRequest are the ones which have no event listeners registered on the object returned by the XMLHttpRequest upload property and have no ReadableStream object used in the request. **CVE ID : CVE-2022-4147**	https://access.redhat.com/security/cve/CVE-2022-4147	A-QUA-QUAR-191222/620
Affected Version(s): From (including) 2.14.0 Up to (excluding) 2.14.2					
N/A	06-Dec-2022	7.5	Quarkus CORS filter allows simple GET and POST requests with invalid Origin to proceed. Simple GET or POST requests made with XMLHttpRequest are the ones which have no event listeners registered on the object returned by the XMLHttpRequest	https://access.redhat.com/security/cve/CVE-2022-4147	A-QUA-QUAR-191222/621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upload property and have no ReadableStream object used in the request. **CVE ID : CVE-2022-4147**		
Vendor: rackn					
Product: digital_rebar					
Affected Version(s): * Up to (including) 4.6.14					
N/A	06-Dec-2022	9.8	RackN Digital Rebar through 4.6.14, 4.7 through 4.7.22, 4.8 through 4.8.5, 4.9 through 4.9.12, and 4.10 through 4.10.8 has exposed a privileged token via a public API endpoint (Incorrect Access Control). The token can be used to escalate privileges within the Digital Rebar system and grant full administrative access. **CVE ID : CVE-2022-46383**	https://docs.rackn.io/en/latest/doc/security/cve_2022_46383.html, https://rackn.com/products/rebar/	A-RAC-DIGI-191222/622
Incorrect Default Permissions	06-Dec-2022	8.8	RackN Digital Rebar through 4.6.14, 4.7 through 4.7.22, 4.8 through 4.8.5, 4.9 through 4.9.12, and 4.10 through 4.10.8 has Insecure Permissions. After signing into Digital Rebar, users are issued authentication tokens tied to their account to perform actions within Digital Rebar. During the validation process of these tokens, Digital Rebar did not check if the	N/A	A-RAC-DIGI-191222/623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user account still exists. Deleted Digital Rebar users could still use their tokens to perform actions within Digital Rebar. **CVE ID : CVE-2022-46382**		
Affected Version(s): From (including) 4.10 Up to (including) 4.10.8					
N/A	06-Dec-2022	9.8	RackN Digital Rebar through 4.6.14, 4.7 through 4.7.22, 4.8 through 4.8.5, 4.9 through 4.9.12, and 4.10 through 4.10.8 has exposed a privileged token via a public API endpoint (Incorrect Access Control). The token can be used to escalate privileges within the Digital Rebar system and grant full administrative access. **CVE ID : CVE-2022-46383**	https://docs.rackn.io/en/latest/doc/security/cve_2022_46383.html, https://rackn.com/products/rebar/	A-RAC-DIGI-191222/624
Incorrect Default Permissions	06-Dec-2022	8.8	RackN Digital Rebar through 4.6.14, 4.7 through 4.7.22, 4.8 through 4.8.5, 4.9 through 4.9.12, and 4.10 through 4.10.8 has Insecure Permissions. After signing into Digital Rebar, users are issued authentication tokens tied to their account to perform actions within Digital Rebar. During the validation process of these tokens, Digital Rebar did not check if the	N/A	A-RAC-DIGI-191222/625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user account still exists. Deleted Digital Rebar users could still use their tokens to perform actions within Digital Rebar. **CVE ID : CVE-2022-46382**		
Affected Version(s): From (including) 4.7 Up to (including) 4.7.22					
N/A	06-Dec-2022	9.8	RackN Digital Rebar through 4.6.14, 4.7 through 4.7.22, 4.8 through 4.8.5, 4.9 through 4.9.12, and 4.10 through 4.10.8 has exposed a privileged token via a public API endpoint (Incorrect Access Control). The token can be used to escalate privileges within the Digital Rebar system and grant full administrative access. **CVE ID : CVE-2022-46383**	https://docs.rackn.io/en/latest/doc/security/cve_2022_46383.html, https://rackn.com/products/rebar/	A-RAC-DIGI-191222/626
Incorrect Default Permissions	06-Dec-2022	8.8	RackN Digital Rebar through 4.6.14, 4.7 through 4.7.22, 4.8 through 4.8.5, 4.9 through 4.9.12, and 4.10 through 4.10.8 has Insecure Permissions. After signing into Digital Rebar, users are issued authentication tokens tied to their account to perform actions within Digital Rebar. During the validation process of these tokens, Digital Rebar did not check if the	N/A	A-RAC-DIGI-191222/627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user account still exists. Deleted Digital Rebar users could still use their tokens to perform actions within Digital Rebar. **CVE ID : CVE-2022-46382**		
Affected Version(s): From (including) 4.8 Up to (including) 4.8.5					
N/A	06-Dec-2022	9.8	RackN Digital Rebar through 4.6.14, 4.7 through 4.7.22, 4.8 through 4.8.5, 4.9 through 4.9.12, and 4.10 through 4.10.8 has exposed a privileged token via a public API endpoint (Incorrect Access Control). The token can be used to escalate privileges within the Digital Rebar system and grant full administrative access. **CVE ID : CVE-2022-46383**	https://docs.rackn.io/en/latest/doc/security/cve_2022_46383.html, https://rackn.com/products/rebar/	A-RAC-DIGI-191222/628
Incorrect Default Permissions	06-Dec-2022	8.8	RackN Digital Rebar through 4.6.14, 4.7 through 4.7.22, 4.8 through 4.8.5, 4.9 through 4.9.12, and 4.10 through 4.10.8 has Insecure Permissions. After signing into Digital Rebar, users are issued authentication tokens tied to their account to perform actions within Digital Rebar. During the validation process of these tokens, Digital Rebar did not check if the	N/A	A-RAC-DIGI-191222/629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user account still exists. Deleted Digital Rebar users could still use their tokens to perform actions within Digital Rebar. **CVE ID : CVE-2022-46382**		
Affected Version(s): From (including) 4.9 Up to (including) 4.9.12					
N/A	06-Dec-2022	9.8	RackN Digital Rebar through 4.6.14, 4.7 through 4.7.22, 4.8 through 4.8.5, 4.9 through 4.9.12, and 4.10 through 4.10.8 has exposed a privileged token via a public API endpoint (Incorrect Access Control). The token can be used to escalate privileges within the Digital Rebar system and grant full administrative access. **CVE ID : CVE-2022-46383**	https://docs.rackn.io/en/latest/doc/security/cve_2022_46383.html, https://rackn.com/products/rebar/	A-RAC-DIGI-191222/630
Incorrect Default Permissions	06-Dec-2022	8.8	RackN Digital Rebar through 4.6.14, 4.7 through 4.7.22, 4.8 through 4.8.5, 4.9 through 4.9.12, and 4.10 through 4.10.8 has Insecure Permissions. After signing into Digital Rebar, users are issued authentication tokens tied to their account to perform actions within Digital Rebar. During the validation process of these tokens, Digital Rebar did not check if the	N/A	A-RAC-DIGI-191222/631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user account still exists. Deleted Digital Rebar users could still use their tokens to perform actions within Digital Rebar. **CVE ID : CVE-2022-46382**		
Vendor: rack_project					
Product: rack					
Affected Version(s): * Up to (excluding) 2.0.9.1					
N/A	05-Dec-2022	10	A sequence injection vulnerability exists in Rack <2.0.9.1, <2.1.4.1 and <2.2.3.1 which could allow is a possible shell escape in the Lint and CommonLogger components of Rack. **CVE ID : CVE-2022-30123**	N/A	A-RAC-RACK-191222/632
Affected Version(s): From (including) 1.2 Up to (excluding) 2.0.9.1					
Uncontrolled Resource Consumption	05-Dec-2022	7.5	A possible denial of service vulnerability exists in Rack <2.0.9.1, <2.1.4.1 and <2.2.3.1 in the multipart parsing component of Rack. **CVE ID : CVE-2022-30122**	N/A	A-RAC-RACK-191222/633
Affected Version(s): From (including) 2.1.0 Up to (excluding) 2.1.4.1					
Uncontrolled Resource Consumption	05-Dec-2022	7.5	A possible denial of service vulnerability exists in Rack <2.0.9.1, <2.1.4.1 and <2.2.3.1 in the multipart parsing component of Rack. **CVE ID : CVE-2022-30122**	N/A	A-RAC-RACK-191222/634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Dec-2022	10	A sequence injection vulnerability exists in Rack <2.0.9.1, <2.1.4.1 and <2.2.3.1 which could allow is a possible shell escape in the Lint and CommonLogger components of Rack. **CVE ID : CVE-2022-30123**	N/A	A-RAC-RACK-191222/635
Affected Version(s): From (including) 2.2.0 Up to (excluding) 2.2.3.1					
Uncontrolled Resource Consumption	05-Dec-2022	7.5	A possible denial of service vulnerability exists in Rack <2.0.9.1, <2.1.4.1 and <2.2.3.1 in the multipart parsing component of Rack. **CVE ID : CVE-2022-30122**	N/A	A-RAC-RACK-191222/636
N/A	05-Dec-2022	10	A sequence injection vulnerability exists in Rack <2.0.9.1, <2.1.4.1 and <2.2.3.1 which could allow is a possible shell escape in the Lint and CommonLogger components of Rack. **CVE ID : CVE-2022-30123**	N/A	A-RAC-RACK-191222/637
Vendor: Radare					
Product: radare2					
Affected Version(s): * Up to (excluding) 5.8.0					
Integer Overflow or Wraparound	10-Dec-2022	7.8	Integer Overflow or Wraparound in GitHub repository radareorg/radare2 prior to 5.8.0. **CVE ID : CVE-2022-4398**	https://github.com/radareorg/radare2/commit/b53a1583d05c3a5bfe5fa60da133fe59dfbb02b8, https://huntr.	A-RAD-RADA-191222/638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				dev/bounties/c6f8d3ef-5420-4eba-9a5f-aba5e2b5fea2	
Vendor: Rapid7					
Product: insightvm					
Affected Version(s): * Up to (excluding) 6.6.172					
Download of Code Without Integrity Check	08-Dec-2022	6.5	Rapid7 Nexpose and InsightVM versions prior to 6.6.172 failed to reliably validate the authenticity of update contents. This failure could allow an attacker to provide a malicious update and alter the functionality of Rapid7 Nexpose. The attacker would need some pre-existing mechanism to provide a malicious update, either through a social engineering effort, privileged access to replace downloaded updates in transit, or by performing an Attacker-in-the-Middle attack on the update service itself. **CVE ID : CVE-2022-4261**	https://docs.rapid7.com/release-notes/nexpose/20221207/, https://www.rapid7.com/blog/post/2022/12/7/cve-2022-4261-rapid7-nexpose-update-validation-issue-fixed, https://docs.rapid7.com/release-notes/insightvm/20221207/	A-RAP-INSI-191222/639
Product: nexpose					
Affected Version(s): * Up to (excluding) 6.6.172					
Download of Code Without Integrity Check	08-Dec-2022	6.5	Rapid7 Nexpose and InsightVM versions prior to 6.6.172 failed to reliably validate the authenticity of update contents. This failure could allow an attacker	https://docs.rapid7.com/release-notes/nexpose/20221207/, https://www.rapid7.com/bl	A-RAP-NEXP-191222/640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to provide a malicious update and alter the functionality of Rapid7 Nexpose. The attacker would need some pre-existing mechanism to provide a malicious update, either through a social engineering effort, privileged access to replace downloaded updates in transit, or by performing an Attacker-in-the-Middle attack on the update service itself. **CVE ID : CVE-2022-4261**	og/post/2022/12/7/cve-2022-4261-rapid7-nexpose-update-validation-issue-fixed, https://docs.rapid7.com/release-notes/insightvm/20221207/	
Vendor: rapidscada					
Product: rapid_scada					
Affected Version(s): 5.8.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-2022	6.1	Rapid Software LLC Rapid SCADA 5.8.4 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2022-44153**	N/A	A-RAP-RAPI-191222/641
Vendor: Redhat					
Product: openshift					
Affected Version(s): 4.9					
Insecure Default Initialization of Resource	08-Dec-2022	8.1	A flaw was found in Openshift. A pod with a DNSPolicy of "ClusterFirst" may incorrectly resolve the hostname based on a service provided. This flaw allows an attacker to supply an incorrect	https://bugzilla.redhat.com/show_bug.cgi?id=2128858	A-RED-OPEN-191222/642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			name with the DNS search policy, affecting confidentiality and availability. **CVE ID : CVE-2022-3262**		
Improper Initialization	09-Dec-2022	7.4	Openshift 4.9 does not use HTTP Strict Transport Security (HSTS) which may allow man-in-the-middle (MITM) attacks. **CVE ID : CVE-2022-3259**	N/A	A-RED-OPEN-191222/643
Improper Restriction of Rendered UI Layers or Frames	08-Dec-2022	4.8	The response header has not enabled X-FRAME-OPTIONS, Which helps prevents against Clickjacking attack.. Some browsers would interpret these results incorrectly, allowing clickjacking attacks. **CVE ID : CVE-2022-3260**	https://bugzilla.redhat.com/show_bug.cgi?id=2106780	A-RED-OPEN-191222/644
Vendor: Redmine					
Product: redmine					
Affected Version(s): * Up to (excluding) 4.2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	6.1	Redmine before 4.2.9 and 5.0.x before 5.0.4 allows persistent XSS in its Textile formatter due to improper sanitization of the blockquote syntax in Textile-formatted fields. **CVE ID : CVE-2022-44031**	https://www.redmine.org/projects/redmine/wiki/Security_Advisories	A-RED-REDM-191222/645
Improper Neutralizat	12-Dec-2022	6.1	Redmine before 4.2.9 and 5.0.x before 5.0.4	https://www.redmine.org/	A-RED-REDM-191222/646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			allows persistent XSS in its Textile formatter due to improper sanitization in Redcloth3 Textile-formatted fields. Depending on the configuration, this may require login as a registered user. **CVE ID : CVE-2022-44637**	projects/redmine/wiki/Security_Advisories	
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	6.1	Redmine before 4.2.9 and 5.0.x before 5.0.4 allows persistent XSS in its Textile formatter due to improper sanitization of the blockquote syntax in Textile-formatted fields. **CVE ID : CVE-2022-44031**	https://www.redmine.org/projects/redmine/wiki/Security_Advisories	A-RED-REDM-191222/647
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	6.1	Redmine before 4.2.9 and 5.0.x before 5.0.4 allows persistent XSS in its Textile formatter due to improper sanitization in Redcloth3 Textile-formatted fields. Depending on the configuration, this may require login as a registered user. **CVE ID : CVE-2022-44637**	https://www.redmine.org/projects/redmine/wiki/Security_Advisories	A-RED-REDM-191222/648
Affected Version(s): From (including) 5.0.0 Up to (including) 5.0.3					
Improper Handling of Exceptiona	06-Dec-2022	7.5	Redmine 5.x before 5.0.4 allows downloading of file attachments of any Issue or any Wiki page due to insufficient	https://www.redmine.org/projects/redmine/wiki/Security_Adviso	A-RED-REDM-191222/649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			permission checks. Depending on the configuration, this may require login as a registered user. **CVE ID : CVE-2022-44030**	ries, https://www.redmine.org/news/139	
Vendor: Rocketsoftware					
Product: trufusion					
Affected Version(s): * Up to (excluding) 7.9.6.1					
Unrestricted Upload of File with Dangerous Type	01-Dec-2022	9.8	An arbitrary file upload vulnerability in Rocket TRUfusion Enterprise before 7.9.6.1 allows unauthenticated attackers to execute arbitrary code via a crafted JSP file. Issue fixed in version 7.9.6.1. **CVE ID : CVE-2022-36431**	https://docs.rocketsoftware.com/bundle/TRUfusionEnterprise_ReleaseNotes_V7.9.6.1/resource/TRUfusionEnterprise_ReleaseNotes_V7.9.6.1.pdf	A-ROC-TRUF-191222/650
Vendor: rukovoditel					
Product: rukovoditel					
Affected Version(s): 3.2.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-2022	9.8	Rukovoditel v3.2.1 was discovered to contain a SQL injection vulnerability via the heading_field_id parameter. **CVE ID : CVE-2022-44945**	N/A	A-RUK-RUKO-191222/651
Improper Neutralization of Input During Web Page	05-Dec-2022	8.8	Rukovoditel v3.2.1 was discovered to contain a DOM-based cross-site scripting (XSS) vulnerability in the component	N/A	A-RUK-RUKO-191222/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			/rukovoditel/index.php?module=users/login. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted GET request. **CVE ID : CVE-2022-45020**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	5.4	Rukovoditel v3.2.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the Add Announcement function at /index.php?module=help_pages/pages&entities_id=24. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Title field. **CVE ID : CVE-2022-44944**	N/A	A-RUK-RUKO-191222/653
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	5.4	Rukovoditel v3.2.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the Add Page function at /index.php?module=help_pages/pages&entities_id=24. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Title field. **CVE ID : CVE-2022-44946**	N/A	A-RUK-RUKO-191222/654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	5.4	Rukovoditel v3.2.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the Highlight Row feature at /index.php?module=entities/listing_types&entities_id=24. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Note field after clicking "Add". **CVE ID : CVE-2022-44947**	N/A	A-RUK-RUKO-191222/655
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	5.4	Rukovoditel v3.2.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the Entities Group feature at/index.php?module=entities/entities_groups. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field after clicking "Add". **CVE ID : CVE-2022-44948**	N/A	A-RUK-RUKO-191222/656
Improper Neutralization of Input During Web Page Generation	02-Dec-2022	5.4	Rukovoditel v3.2.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the Add New Field function at /index.php?module=entities/fields&entities_id=2	N/A	A-RUK-RUKO-191222/657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			4. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Short Name field. **CVE ID : CVE-2022-44949**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	5.4	Rukovoditel v3.2.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the Add New Field function at /index.php?module=entities/fields&entities_id=24. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2022-44950**	N/A	A-RUK-RUKO-191222/658
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	5.4	Rukovoditel v3.2.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the Add New Form tab function at /index.php?module=entities/forms&entities_id=24. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2022-44951**	N/A	A-RUK-RUKO-191222/659
Improper Neutralizat	02-Dec-2022	5.4	Rukovoditel v3.2.1 was discovered to contain a	N/A	A-RUK-RUKO-191222/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			stored cross-site scripting (XSS) vulnerability in /index.php?module=configuration/application. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Copyright Text field after clicking "Add". **CVE ID : CVE-2022-44952**		
Vendor: ruoyi					
Product: ruoyi-cloud					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Dec-2022	6.1	A vulnerability was found in y_project RuoYi-Cloud. It has been rated as problematic. Affected by this issue is some unknown functionality of the component JSON Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-215108. **CVE ID : CVE-2022-4348**	N/A	A-RUO-RUOY-191222/661
Vendor: rxvt-unicode_project					
Product: rxvt-unicode					
Affected Version(s): 9.25					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	09-Dec-2022	9.8	The rxvt-unicode package is vulnerable to a remote code execution, in the Perl background extension, when an attacker can control the data written to the user's terminal and certain options are set. **CVE ID : CVE-2022-4170**	N/A	A-RXV-RXVT-191222/662
Affected Version(s): 9.26					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	09-Dec-2022	9.8	The rxvt-unicode package is vulnerable to a remote code execution, in the Perl background extension, when an attacker can control the data written to the user's terminal and certain options are set. **CVE ID : CVE-2022-4170**	N/A	A-RXV-RXVT-191222/663
Vendor: S-cms					
Product: S-cms					
Affected Version(s): 5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-2022	5.4	A vulnerability was found in S-CMS 5.0 Build 20220328. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Contact Information Page. The manipulation of the argument Make a Call leads to cross site	N/A	A-S-C-S-CM-191222/664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-215197 was assigned to this vulnerability. **CVE ID : CVE-2022-4377**		
Vendor: salonbookingsystem					
Product: salon_booking_system					
Affected Version(s): * Up to (excluding) 7.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	6.1	Cross-site scripting vulnerability in Salon booking system versions prior to 7.9 allows a remote unauthenticated attacker to inject an arbitrary script. **CVE ID : CVE-2022-43487**	https://www.salonbookingsystem.com/	A-SAL-SALO-191222/665
Vendor: Samsung					
Product: calendar					
Affected Version(s): * Up to (excluding) 11.6.08.0					
N/A	08-Dec-2022	5.5	Improper access control vulnerability in Calendar prior to versions 11.6.08.0 in Android Q(10), 12.2.11.3000 in Android R(11), 12.3.07.2000 in Android S(12), and 12.4.02.0 in Android T(13) allows attackers to access sensitive information via implicit intent. **CVE ID : CVE-2022-39915**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=12	A-SAM-CALE-191222/666
Affected Version(s): * Up to (excluding) 12.2.11.3000					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Dec-2022	5.5	Improper access control vulnerability in Calendar prior to versions 11.6.08.0 in Android Q(10), 12.2.11.3000 in Android R(11), 12.3.07.2000 in Android S(12), and 12.4.02.0 in Android T(13) allows attackers to access sensitive information via implicit intent. **CVE ID : CVE-2022-39915**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=12	A-SAM-CALE-191222/667
Affected Version(s): * Up to (excluding) 12.3.07.2000					
N/A	08-Dec-2022	5.5	Improper access control vulnerability in Calendar prior to versions 11.6.08.0 in Android Q(10), 12.2.11.3000 in Android R(11), 12.3.07.2000 in Android S(12), and 12.4.02.0 in Android T(13) allows attackers to access sensitive information via implicit intent. **CVE ID : CVE-2022-39915**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=12	A-SAM-CALE-191222/668
Affected Version(s): * Up to (excluding) 12.4.02.0					
N/A	08-Dec-2022	5.5	Improper access control vulnerability in Calendar prior to versions 11.6.08.0 in Android Q(10), 12.2.11.3000 in Android R(11), 12.3.07.2000 in Android S(12), and 12.4.02.0 in Android T(13) allows attackers to access sensitive information via implicit intent.	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=12	A-SAM-CALE-191222/669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39915		
Product: gear_iconx_pc_manager					
Affected Version(s): * Up to (excluding) 2.1.221019.51					
Insufficient Verification of Data Authenticity	08-Dec-2022	5.5	Insufficient verification of data authenticity vulnerability in Samsung Gear IconX PC Manager prior to version 2.1.221019.51 allows local attackers to create arbitrary file using symbolic link. **CVE ID : CVE-2022-39909**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=12	A-SAM-GEAR-191222/670
Product: pass					
Affected Version(s): * Up to (excluding) 4.0.06.1					
N/A	08-Dec-2022	6.8	Improper check or handling of exceptional conditions vulnerability in Samsung Pass prior to version 4.0.06.1 allows attacker to access Samsung Pass. **CVE ID : CVE-2022-39911**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=12	A-SAM-PASS-191222/671
Affected Version(s): * Up to (excluding) 4.0.06.7					
N/A	08-Dec-2022	4.2	Improper access control vulnerability in Samsung Pass prior to version 4.0.06.7 allow physical attackers to access data of Samsung Pass on a certain state of an unlocked device using pop-up view. **CVE ID : CVE-2022-39910**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=12	A-SAM-PASS-191222/672
Vendor: Sangoma					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: asterisk					
Affected Version(s): 20.0.0					
Out-of-bounds Write	05-Dec-2022	7.5	In Sangoma Asterisk through 16.28.0, 17.x and 18.x through 18.14.0, and 19.x through 19.6.0, an incoming Setup message to addons/ooh323c/src/ooq931.c with a malformed Calling or Called Party IE can cause a crash. **CVE ID : CVE-2022-37325**	https://downloads.asterisk.org/pub/security/AST-2022-007.html	A-SAN-ASTE-191222/673
Use After Free	05-Dec-2022	6.5	A use-after-free in res_pjsip_pubsub.c in Sangoma Asterisk 16.28, 18.14, 19.6, and certified/18.9-cert2 may allow a remote authenticated attacker to crash Asterisk (denial of service) by performing activity on a subscription via a reliable transport at the same time that Asterisk is also performing activity on that subscription. **CVE ID : CVE-2022-42705**	https://downloads.asterisk.org/pub/security/AST-2022-008.html	A-SAN-ASTE-191222/674
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Dec-2022	4.9	An issue was discovered in Sangoma Asterisk through 16.28, 17 and 18 through 18.14, 19 through 19.6, and certified through 18.9-cert1. GetConfig, via Asterisk Manager Interface, allows a connected application to access files outside of the	https://downloads.asterisk.org/pub/security/AST-2022-009.html	A-SAN-ASTE-191222/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			asterisk configuration directory, aka Directory Traversal. **CVE ID : CVE-2022-42706**		
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.29.1					
Out-of-bounds Write	05-Dec-2022	7.5	In Sangoma Asterisk through 16.28.0, 17.x and 18.x through 18.14.0, and 19.x through 19.6.0, an incoming Setup message to addons/ooh323c/src/ooq931.c with a malformed Calling or Called Party IE can cause a crash. **CVE ID : CVE-2022-37325**	https://downloads.asterisk.org/pub/security/AST-2022-007.html	A-SAN-ASTE-191222/676
Use After Free	05-Dec-2022	6.5	A use-after-free in res_pjsip_pubsub.c in Sangoma Asterisk 16.28, 18.14, 19.6, and certified/18.9-cert2 may allow a remote authenticated attacker to crash Asterisk (denial of service) by performing activity on a subscription via a reliable transport at the same time that Asterisk is also performing activity on that subscription. **CVE ID : CVE-2022-42705**	https://downloads.asterisk.org/pub/security/AST-2022-008.html	A-SAN-ASTE-191222/677
Improper Limitation of a Pathname to a Restricted Directory	05-Dec-2022	4.9	An issue was discovered in Sangoma Asterisk through 16.28, 17 and 18 through 18.14, 19 through 19.6, and certified through 18.9-cert1. GetConfig, via	https://downloads.asterisk.org/pub/security/AST-2022-009.html	A-SAN-ASTE-191222/678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			Asterisk Manager Interface, allows a connected application to access files outside of the asterisk configuration directory, aka Directory Traversal. **CVE ID : CVE-2022-42706**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 18.15.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Dec-2022	4.9	An issue was discovered in Sangoma Asterisk through 16.28, 17 and 18 through 18.14, 19 through 19.6, and certified through 18.9-cert1. GetConfig, via Asterisk Manager Interface, allows a connected application to access files outside of the asterisk configuration directory, aka Directory Traversal. **CVE ID : CVE-2022-42706**	https://downloads.asterisk.org/pub/security/AST-2022-009.html	A-SAN-ASTE-191222/679
Affected Version(s): From (including) 18.0.0 Up to (excluding) 18.15.1					
Out-of-bounds Write	05-Dec-2022	7.5	In Sangoma Asterisk through 16.28.0, 17.x and 18.x through 18.14.0, and 19.x through 19.6.0, an incoming Setup message to addons/ooh323c/src/ooq931.c with a malformed Calling or Called Party IE can cause a crash. **CVE ID : CVE-2022-37325**	https://downloads.asterisk.org/pub/security/AST-2022-007.html	A-SAN-ASTE-191222/680
Affected Version(s): From (including) 18.14.0 Up to (excluding) 18.15.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	05-Dec-2022	6.5	A use-after-free in res_pjsip_pubsub.c in Sangoma Asterisk 16.28, 18.14, 19.6, and certified/18.9-cert2 may allow a remote authenticated attacker to crash Asterisk (denial of service) by performing activity on a subscription via a reliable transport at the same time that Asterisk is also performing activity on that subscription. **CVE ID : CVE-2022-42705**	https://downloads.asterisk.org/pub/security/AST-2022-008.html	A-SAN-ASTE-191222/681
Affected Version(s): From (including) 19.0.0 Up to (excluding) 19.7.1					
Out-of-bounds Write	05-Dec-2022	7.5	In Sangoma Asterisk through 16.28.0, 17.x and 18.x through 18.14.0, and 19.x through 19.6.0, an incoming Setup message to addons/ooh323c/src/ooq931.c with a malformed Calling or Called Party IE can cause a crash. **CVE ID : CVE-2022-37325**	https://downloads.asterisk.org/pub/security/AST-2022-007.html	A-SAN-ASTE-191222/682
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Dec-2022	4.9	An issue was discovered in Sangoma Asterisk through 16.28, 17 and 18 through 18.14, 19 through 19.6, and certified through 18.9-cert1. GetConfig, via Asterisk Manager Interface, allows a connected application to access files outside of the asterisk configuration	https://downloads.asterisk.org/pub/security/AST-2022-009.html	A-SAN-ASTE-191222/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			directory, aka Directory Traversal. **CVE ID : CVE-2022-42706**		
Affected Version(s): From (including) 19.6.0 Up to (excluding) 19.7.1					
Use After Free	05-Dec-2022	6.5	A use-after-free in res_pjsip_pubsub.c in Sangoma Asterisk 16.28, 18.14, 19.6, and certified/18.9-cert2 may allow a remote authenticated attacker to crash Asterisk (denial of service) by performing activity on a subscription via a reliable transport at the same time that Asterisk is also performing activity on that subscription. **CVE ID : CVE-2022-42705**	https://downloads.asterisk.org/pub/security/AST-2022-008.html	A-SAN-ASTE-191222/684
Product: certified_asterisk					
Affected Version(s): * Up to (excluding) 18.9					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Dec-2022	4.9	An issue was discovered in Sangoma Asterisk through 16.28, 17 and 18 through 18.14, 19 through 19.6, and certified through 18.9-cert1. GetConfig, via Asterisk Manager Interface, allows a connected application to access files outside of the asterisk configuration directory, aka Directory Traversal. **CVE ID : CVE-2022-42706**	https://downloads.asterisk.org/pub/security/AST-2022-009.html	A-SAN-CERT-191222/685
Affected Version(s): 18.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	05-Dec-2022	6.5	A use-after-free in res_pjsip_pubsub.c in Sangoma Asterisk 16.28, 18.14, 19.6, and certified/18.9-cert2 may allow a remote authenticated attacker to crash Asterisk (denial of service) by performing activity on a subscription via a reliable transport at the same time that Asterisk is also performing activity on that subscription. **CVE ID : CVE-2022-42705**	https://downloads.asterisk.org/pub/security/AST-2022-008.html	A-SAN-CERT-191222/686
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Dec-2022	4.9	An issue was discovered in Sangoma Asterisk through 16.28, 17 and 18 through 18.14, 19 through 19.6, and certified through 18.9-cert1. GetConfig, via Asterisk Manager Interface, allows a connected application to access files outside of the asterisk configuration directory, aka Directory Traversal. **CVE ID : CVE-2022-42706**	https://downloads.asterisk.org/pub/security/AST-2022-009.html	A-SAN-CERT-191222/687
Vendor: sanitization_management_system_project					
Product: sanitization_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an	02-Dec-2022	7.2	Sanitization Management System v1.0 is vulnerable to SQL Injection via /php-	N/A	A-SAN-SANI-191222/688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			sms/classes/Master.php?f=delete_product. **CVE ID : CVE-2022-44277**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-2022	7.2	Sanitization Management System v1.0 is vulnerable to SQL Injection via /php-sms/admin/?page=quotes/view_quote&id=. **CVE ID : CVE-2022-44345**	N/A	A-SAN-SANI-191222/689
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-2022	7.2	Sanitization Management System v1.0 is vulnerable to SQL Injection via /php-sms/admin/?page=inquiries/view_inquiry&id=. **CVE ID : CVE-2022-44347**	N/A	A-SAN-SANI-191222/690
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-2022	7.2	Sanitization Management System v1.0 is vulnerable to SQL Injection via /php-sms/admin/orders/update_status.php?id=. **CVE ID : CVE-2022-44348**	N/A	A-SAN-SANI-191222/691
Improper Neutralization of Special Elements used in an SQL Command	07-Dec-2022	7.2	Sanitization Management System v1.0 is vulnerable to SQL Injection via /php-sms/admin/?page=services/view_service&id=. **CVE ID : CVE-2022-44393**	N/A	A-SAN-SANI-191222/692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')					
Vendor: SAP					
Product: business_objects_business_intelligence_platform					
Affected Version(s): 430					
N/A	12-Dec-2022	6	Under certain conditions, an attacker authenticated as a CMS administrator and with high privileges access to the Network in SAP BusinessObjects Business Intelligence Platform (Monitoring DB) - version 430, can access BOE Monitoring database to retrieve and modify (non-personal) system data which would otherwise be restricted. Also, a potential attack could be used to leave the CMS's scope and impact the database. A successful attack could have a low impact on confidentiality, a high impact on integrity, and a low impact on availability. **CVE ID : CVE-2022-31596**	https://launchpad.support.sap.com/#/notes/3213507, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-191222/693
Vendor: secomea					
Product: gatemanager					
Affected Version(s): * Up to (excluding) 10.0.622395010					
Improper Input Validation	06-Dec-2022	7.2	Improper Input Validation of plugin files in Administrator Interface of Secomea GateManager allows a server administrator to inject code into the	https://www.secomea.com/support/cybersecurity-advisory/	A-SEC-GATE-191222/694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GateManager interface. This issue affects: Secomea GateManager versions prior to 10.0. **CVE ID : CVE-2022-38123**		
Affected Version(s): From (including) 9.4 Up to (including) 9.7					
Improper Authentication	09-Dec-2022	7.8	A vulnerability in the web server of Secomea GateManager allows a local user to impersonate as the previous user under some failed login conditions. This issue affects: Secomea GateManager versions from 9.4 through 9.7. **CVE ID : CVE-2022-2752**	https://www.secomea.com/support/cybersecurity-advisory	A-SEC-GATE-191222/695
Vendor: Seeddms					
Product: seeddms					
Affected Version(s): 5.1.7					
N/A	08-Dec-2022	9.8	Weak reset token generation in SeedDMS v6.0.20 and v5.1.7 allows attackers to execute a full account takeover via a brute force attack. **CVE ID : CVE-2022-44938**	N/A	A-SEE-SEED-191222/696
Affected Version(s): 6.0.20					
N/A	08-Dec-2022	9.8	Weak reset token generation in SeedDMS v6.0.20 and v5.1.7 allows attackers to execute a full account takeover via a brute force attack. **CVE ID : CVE-2022-44938**	N/A	A-SEE-SEED-191222/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: sens_project					
Product: sens					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	12-Dec-2022	8.8	SENS v1.0 has a file upload vulnerability. **CVE ID : CVE-2022-45759**	N/A	A-SEN-SENS-191222/698
Incorrect Authorization	12-Dec-2022	8.8	SENS v1.0 is vulnerable to Incorrect Access Control vulnerability. **CVE ID : CVE-2022-45760**	N/A	A-SEN-SENS-191222/699
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	6.1	SENS v1.0 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2022-45756**	N/A	A-SEN-SENS-191222/700
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	5.4	SENS v1.0 is vulnerable to Cross Site Scripting (XSS) via com.liuyanzhao.sens.web.controller.admin, getRegister. **CVE ID : CVE-2022-45758**	N/A	A-SEN-SENS-191222/701
Vendor: sentry					
Product: sentry					
Affected Version(s): From (including) 20.6.0 Up to (including) 22.10.0					
Improper Privilege Management	10-Dec-2022	3.7	Sentry is an error tracking and performance monitoring platform. In versions of the sentry python library prior to 22.11.0 an	N/A	A-SEN-SENT-191222/702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with a known valid invite link could manipulate a cookie to allow the same invite link to be reused on multiple accounts when joining an organization. As a result an attacker with a valid invite link can create multiple users and join an organization they may not have been originally invited to. This issue was patched in version 22.11.0. Sentry SaaS customers do not need to take action. Self-hosted Sentry installs on systems which can not upgrade can disable the invite functionality until they are ready to deploy the patched version by editing their `sentry.conf.py` file (usually located at `~/.sentry/`). **CVE ID : CVE-2022-23485**		
Vendor: shift-tech					
Product: bingo\!cms					
Affected Version(s): * Up to (including) 1.7.4.1					
Missing Authentication for Critical Function	07-Dec-2022	9.8	Authentication bypass using an alternate path or channel vulnerability in bingo!CMS version1.7.4.1 and earlier allows a remote unauthenticated attacker to upload an arbitrary file. As a result, an arbitrary script may be	https://www.bingo-cms.jp/information/20221011.html	A-SHI-BING-191222/703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed and/or a file may be altered. **CVE ID : CVE-2022-42458**		
Vendor: simple-git_project					
Product: simple-git					
Affected Version(s): * Up to (excluding) 3.15.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Dec-2022	9.8	The package simple-git before 3.15.0 are vulnerable to Remote Code Execution (RCE) when enabling the ext transport protocol, which makes it exploitable via clone() method. This vulnerability exists due to an incomplete fix of [CVE-2022-24066](https://security.snyk.io/vuln/SNYK-JS-SIMPLEGIT-2434306). **CVE ID : CVE-2022-25912**	https://github.com/steveukx/git-js/commit/774648049eb3e628379e292ea172dccaba610504, https://github.com/steveukx/git-js/releases/tag/simple-git%403.15.0, https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-3153532	A-SIM-SIMP-191222/704
Vendor: simple_phone_book\/directory_web_app_project					
Product: simple_phone_book\/directory_web_app					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Dec-2022	9.8	Simple Phone Book/Directory Web App v1.0 was discovered to contain a SQL injection vulnerability via the editid parameter at /PhoneBook/edit.php. **CVE ID : CVE-2022-45010**	N/A	A-SIM-SIMP-191222/705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Sixapart					
Product: movable_type					
Affected Version(s): * Up to (including) 1.53					
Improper Control of Generation of Code ('Code Injection')	07-Dec-2022	7.2	Improper neutralization of Server-Side Includes (SSW) within a web page in Movable Type series allows a remote authenticated attacker with Privilege of 'Manage of Content Types' may execute an arbitrary Perl script and/or an arbitrary OS command. Affected products/versions are as follows: Movable Type 7 r.5301 and earlier (Movable Type 7 Series), Movable Type Advanced 7 r.5301 and earlier (Movable Type Advanced 7 Series), Movable Type Premium 1.53 and earlier, and Movable Type Premium Advanced 1.53 and earlier. **CVE ID : CVE-2022-43660**	https://movabletype.org/news/2022/11/mt-796-688-released.html	A-SIX-MOVA-191222/706
Improper Input Validation	07-Dec-2022	6.5	Improper validation of syntactic correctness of input vulnerability exist in Movable Type series. Having a user to access a specially crafted URL may allow a remote unauthenticated attacker to set a specially crafted URL to the Reset Password page and conduct a phishing attack. Affected	https://movabletype.org/news/2022/11/mt-796-688-released.html	A-SIX-MOVA-191222/707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products/versions are as follows: Movable Type 7 r.5301 and earlier (Movable Type 7 Series), Movable Type Advanced 7 r.5301 and earlier (Movable Type Advanced 7 Series), Movable Type 6.8.7 and earlier (Movable Type 6 Series), Movable Type Advanced 6.8.7 and earlier (Movable Type Advanced 6 Series), Movable Type Premium 1.53 and earlier, and Movable Type Premium Advanced 1.53 and earlier. **CVE ID : CVE-2022-45113**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-2022	6.1	Cross-site scripting vulnerability in Movable Type Movable Type 7 r.5301 and earlier (Movable Type 7 Series), Movable Type Advanced 7 r.5301 and earlier (Movable Type Advanced 7 Series), Movable Type 6.8.7 and earlier (Movable Type 6 Series), Movable Type Advanced 6.8.7 and earlier (Movable Type Advanced 6 Series), Movable Type Premium 1.53 and earlier, and Movable Type Premium Advanced 1.53 and earlier allows a remote unauthenticated attacker to inject an arbitrary script.	https://movabletype.org/news/2022/11/mt-796-688-released.html	A-SIX-MOVA-191222/708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45122		
Affected Version(s): From (including) 6.0 Up to (excluding) 6.8.7					
Improper Input Validation	07-Dec-2022	6.5	Improper validation of syntactic correctness of input vulnerability exist in Movable Type series. Having a user to access a specially crafted URL may allow a remote unauthenticated attacker to set a specially crafted URL to the Reset Password page and conduct a phishing attack. Affected products/versions are as follows: Movable Type 7 r.5301 and earlier (Movable Type 7 Series), Movable Type Advanced 7 r.5301 and earlier (Movable Type Advanced 7 Series), Movable Type 6.8.7 and earlier (Movable Type 6 Series), Movable Type Advanced 6.8.7 and earlier (Movable Type Advanced 6 Series), Movable Type Premium 1.53 and earlier, and Movable Type Premium Advanced 1.53 and earlier. **CVE ID : CVE-2022-45113**	https://movabletype.org/news/2022/11/mt-796-688-released.html	A-SIX-MOVA-191222/709
Improper Neutralization of Input During Web Page Generation	07-Dec-2022	6.1	Cross-site scripting vulnerability in Movable Type Movable Type 7 r.5301 and earlier (Movable Type 7 Series), Movable Type Advanced 7 r.5301 and earlier	https://movabletype.org/news/2022/11/mt-796-688-released.html	A-SIX-MOVA-191222/710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			(Movable Type Advanced 7 Series), Movable Type 6.8.7 and earlier (Movable Type 6 Series), Movable Type Advanced 6.8.7 and earlier (Movable Type Advanced 6 Series), Movable Type Premium 1.53 and earlier, and Movable Type Premium Advanced 1.53 and earlier allows a remote unauthenticated attacker to inject an arbitrary script. **CVE ID : CVE-2022-45122**		
Affected Version(s): From (including) 7.0 Up to (excluding) 7.9.6					
Improper Control of Generation of Code ('Code Injection')	07-Dec-2022	7.2	Improper neutralization of Server-Side Includes (SSW) within a web page in Movable Type series allows a remote authenticated attacker with Privilege of 'Manage of Content Types' may execute an arbitrary Perl script and/or an arbitrary OS command. Affected products/versions are as follows: Movable Type 7 r.5301 and earlier (Movable Type 7 Series), Movable Type Advanced 7 r.5301 and earlier (Movable Type Advanced 7 Series), Movable Type Premium 1.53 and earlier, and Movable Type Premium Advanced 1.53 and earlier.	https://movabletype.org/news/2022/11/mt-796-688-released.html	A-SIX-MOVA-191222/711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43660		
Improper Input Validation	07-Dec-2022	6.5	Improper validation of syntactic correctness of input vulnerability exist in Movable Type series. Having a user to access a specially crafted URL may allow a remote unauthenticated attacker to set a specially crafted URL to the Reset Password page and conduct a phishing attack. Affected products/versions are as follows: Movable Type 7 r.5301 and earlier (Movable Type 7 Series), Movable Type Advanced 7 r.5301 and earlier (Movable Type Advanced 7 Series), Movable Type 6.8.7 and earlier (Movable Type 6 Series), Movable Type Advanced 6.8.7 and earlier (Movable Type Advanced 6 Series), Movable Type Premium 1.53 and earlier, and Movable Type Premium Advanced 1.53 and earlier. **CVE ID : CVE-2022-45113**	https://movabletype.org/news/2022/11/mt-796-688-released.html	A-SIX-MOVA-191222/712
Improper Neutralization of Input During Web Page Generation	07-Dec-2022	6.1	Cross-site scripting vulnerability in Movable Type Movable Type 7 r.5301 and earlier (Movable Type 7 Series), Movable Type Advanced 7 r.5301 and earlier (Movable Type Advanced	https://movabletype.org/news/2022/11/mt-796-688-released.html	A-SIX-MOVA-191222/713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			7 Series), Movable Type 6.8.7 and earlier (Movable Type 6 Series), Movable Type Advanced 6.8.7 and earlier (Movable Type Advanced 6 Series), Movable Type Premium 1.53 and earlier, and Movable Type Premium Advanced 1.53 and earlier allows a remote unauthenticated attacker to inject an arbitrary script. **CVE ID : CVE-2022-45122**		
Vendor: skycaiji					
Product: skycaiji					
Affected Version(s): 2.5.1					
Deserialization of Untrusted Data	07-Dec-2022	9.8	Skycaiji v2.5.1 was discovered to contain a deserialization vulnerability via /SkycaijiApp/admin/controller/Mystore.php. **CVE ID : CVE-2022-44351**	N/A	A-SKY-SKYC-191222/714
Vendor: Slims					
Product: senayan_library_management_system					
Affected Version(s): 9.5.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Dec-2022	7.5	SLiMS 9 Bulian v9.5.0 was discovered to contain a SQL injection vulnerability via the keywords parameter. **CVE ID : CVE-2022-45019**	N/A	A-SLI-SENA-191222/715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: snakeyaml_project					
Product: snakeyaml					
Affected Version(s): 1.30					
Deserialization of Untrusted Data	01-Dec-2022	9.8	SnakeYaml's Constructor() class does not restrict types which can be instantiated during deserialization. Deserializing yaml content provided by an attacker can lead to remote code execution. We recommend using SnakeYaml's SafeConsturctor when parsing untrusted content to restrict deserialization. **CVE ID : CVE-2022-1471**	N/A	A-SNA-SNAK-191222/716
Vendor: Sqlite					
Product: sqlite					
Affected Version(s): * Up to (including) 3.40.0					
N/A	12-Dec-2022	9.8	SQLite through 3.40.0, when relying on --safe for execution of an untrusted CLI script, does not properly implement the azProhibitedFunctions protection mechanism, and instead allows UDF functions such as WRITEFILE. **CVE ID : CVE-2022-46908**	https://sqlite.org/src/info/cefc032473ac5ad2, https://sqlite.org/forum/forumpost/07beac8056151b2f	A-SQL-SQLI-191222/717
Vendor: ss-proj					
Product: shirasagi					
Affected Version(s): * Up to (excluding) 1.16.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	5.4	Stored cross-site scripting vulnerability in SHIRASAGI versions prior to v1.16.2 allows a remote authenticated attacker with an administrative privilege to inject an arbitrary script. **CVE ID : CVE-2022-43499**	https://www.ss-proj.org/support/928.html, https://www.ss-proj.org/	A-SS--SHIR-191222/718
Affected Version(s): From (including) 1.14.4 Up to (including) 1.15.0					
URL Redirection to Untrusted Site ('Open Redirect')	05-Dec-2022	6.1	Open redirect vulnerability in SHIRASAGI v1.14.4 to v1.15.0 allows a remote unauthenticated attacker to redirect users to an arbitrary web site and conduct a phishing attack. **CVE ID : CVE-2022-43479**	https://www.ss-proj.org/support/928.html, https://www.ss-proj.org/	A-SS--SHIR-191222/719
Vendor: stackstorm					
Product: stackstorm					
Affected Version(s): * Up to (excluding) 3.8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	5.4	Cross-site scripting (XSS) vulnerability in the Web UI of StackStorm versions prior to 3.8.0 allowed logged in users with write access to pack rules to inject arbitrary script or HTML that may be executed in Web UI for other logged in users. **CVE ID : CVE-2022-43706**	https://stackstorm.com/2022/12/v3-8-0-released/	A-STA-STAC-191222/720
Affected Version(s): 3.7.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.5	Improper access control in Key-Value RBAC in StackStorm version 3.7.0 didn't check the permissions in Jinja filters, allowing attackers to access K/V pairs of other users, potentially leading to the exposure of sensitive Information. **CVE ID : CVE-2022-44009**	https://stackstorm.com/2022/12/v3-8-0-released/	A-STA-STAC-191222/721
Vendor: stopbadbots_project					
Product: stopbadbots					
Affected Version(s): * Up to (excluding) 7.24					
Cross-Site Request Forgery (CSRF)	12-Dec-2022	6.5	The Block Bad Bots and Stop Bad Bots Crawlers and Spiders and Anti Spam Protection WordPress plugin before 7.24 does not have proper authorisation and CSRF in an AJAX action, allowing any authenticated users, such as subscriber to call it and install and activate arbitrary plugins from wordpress.org **CVE ID : CVE-2022-3883**	N/A	A-STO-STOP-191222/722
Vendor: supra-csv-parser_project					
Product: supra-csv-parser					
Affected Version(s): * Up to (including) 4.0.3					
Improper Neutralization of Input During Web Page Generation	12-Dec-2022	5.4	Cross-site Scripting (XSS) is a client-side code injection attack. The attacker aims to execute malicious scripts in a web browser of the victim by including	N/A	A-SUP-SUPR-191222/723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			malicious code in a legitimate web page or web application. **CVE ID : CVE-2022-3853**		
Vendor: swiftterm_project					
Product: swiftterm					
Affected Version(s): * Up to (excluding) 2022-12-02					
Improper Control of Generation of Code ('Code Injection')	02-Dec-2022	7.8	SwiftTerm is a Xterm/VT100 Terminal emulator. Prior to commit a94e6b24d24ce9680ad79884992e1dff8e150a31, an attacker could modify the window title via a certain character escape sequence and then insert it back to the command line in the user's terminal, e.g. when the user views a file containing the malicious sequence, which could allow the attacker to execute arbitrary commands. Version a94e6b24d24ce9680ad79884992e1dff8e150a31 contains a patch for this issue. There are no known workarounds available. **CVE ID : CVE-2022-23465**	https://github.com/migueldeicaza/SwiftTerm/commit/a94e6b24d24ce9680ad79884992e1dff8e150a31	A-SWI-SWIF-191222/724
Vendor: Symantec					
Product: messaging_gateway					
Affected Version(s): From (including) 10.7.4 Up to (excluding) 10.8					
Improper Neutralization of	09-Dec-2022	5.4	An authenticated user who has the privilege to add/edit annotations on	https://support.broadcom.com/external/	A-SYM-MESS-191222/725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			the Content tab, can craft a malicious annotation that can be executed on the annotations page (Annotation Text Column) **CVE ID : CVE-2022-25629**	content/SecurityAdvisories/0/21115	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-2022	5.4	An authenticated user can embed malicious content with XSS into the admin group policy page. **CVE ID : CVE-2022-25630**	https://support.broadcom.com/external/content/SecurityAdvisories/0/21117	A-SYM-MESS-191222/726
Vendor: syncee					
Product: syncee_-_global_dropshipping					
Affected Version(s): * Up to (excluding) 1.0.10					
Exposure of Sensitive Information to an Unauthorized Actor	05-Dec-2022	7.5	The Syncee WordPress plugin before 1.0.10 leaks the administrator token that can be used to take over the administrator's account. **CVE ID : CVE-2022-3694**	N/A	A-SYN-SYNC-191222/727
Vendor: Telegram					
Product: telegram					
Affected Version(s): 15.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	** DISPUTED ** Telegram Web 15.3.1 allows XSS via a certain payload derived from a Target Corporation website. NOTE: some third parties have been unable to discern any relationship between the	N/A	A-TEL-TELE-191222/728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Pastebin information and a possible XSS finding. **CVE ID : CVE-2022-43363**		
Vendor: teleniasoftware					
Product: tvox					
Affected Version(s): * Up to (excluding) 22.0.17					
N/A	01-Dec-2022	9.8	Telenia Software s.r.l TVox before v22.0.17 was discovered to contain a remote code execution (RCE) vulnerability in the component action_export_control.php. **CVE ID : CVE-2022-43333**	N/A	A-TEL-TVOX-191222/729
Vendor: telepad-app					
Product: telepad					
Affected Version(s): * Up to (including) 1.0.7					
Missing Authentication for Critical Function	05-Dec-2022	9.8	Telepad allows remote unauthenticated users to send instructions to the server to execute arbitrary code without any previous authorization or authentication. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H **CVE ID : CVE-2022-45477**	https://www.synopsys.com/blogs/software-security/cyrc-advisory-remote-code-execution-vulnerabilities-mouse-keyboard-apps/	A-TEL-TELE-191222/730
Cleartext Transmission of Sensitive Information	05-Dec-2022	5.9	Telepad allows an attacker (in a man-in-the-middle position between the server and a connected device) to see all data (including keypresses) in cleartext.	https://www.synopsys.com/blogs/software-security/cyrc-advisory-remote-code-	A-TEL-TELE-191222/731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N **CVE ID : CVE-2022-45478**	execution-vulnerabilities-mouse-keyboard-apps/	
Vendor: teler_project					
Product: teler					
Affected Version(s): 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	5.4	teler is an real-time intrusion detection and threat alert dashboard. teler prior to version 2.0.0-rc.4 is vulnerable to DOM-based cross-site scripting (XSS) in the teler dashboard. When teler requests messages from the event stream on the `/events` endpoint, the log data displayed on the dashboard are not sanitized. This only affects authenticated users and can only be exploited based on detected threats if the log contains a DOM scripting payload. This vulnerability has been fixed on version `v2.0.0-rc.4`. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2022-23466**	https://github.com/kitabisa/teler/commit/20f59eda2420ac64e29f199a61230a0abc875e8e, https://github.com/kitabisa/teler/security/advisories/GHSA-xr7p-8q82-878q	A-TEL-TELE-191222/732
Vendor: themeum					
Product: wp_page_builder					
Affected Version(s): * Up to (including) 1.2.8					
Improper Neutralizat	05-Dec-2022	4.8	The WP Page Builder WordPress plugin	N/A	A-THE-WP_P-191222/733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			through 1.2.8 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-2022-3830**		
Vendor: themographics					
Product: listingo					
Affected Version(s): * Up to (excluding) 3.2.7					
Unrestricted Upload of File with Dangerous Type	12-Dec-2022	9.8	The Listingo WordPress theme before 3.2.7 does not validate files to be uploaded via an AJAX action available to unauthenticated users, which could allow them to upload arbitrary files and lead to RCE **CVE ID : CVE-2022-3921**	N/A	A-THE-LIST-191222/734
Vendor: Thinkcmf					
Product: Thinkcmf					
Affected Version(s): 6.0.7					
Cross-Site Request Forgery (CSRF)	01-Dec-2022	8.8	ThinkCMF version 6.0.7 is affected by a Cross Site Request Forgery (CSRF) vulnerability that allows a Super Administrator user to be injected into administrative users. **CVE ID : CVE-2022-40489**	N/A	A-THI-THIN-191222/735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-2022	5.4	ThinkCMF version 6.0.7 is affected by Stored Cross-Site Scripting (XSS). An attacker who successfully exploited this vulnerability could inject a Persistent XSS payload in the Slideshow Management section that execute arbitrary JavaScript code on the client side, e.g., to steal the administrator's PHP session token (PHPSESSID). **CVE ID : CVE-2022-40849**	N/A	A-THI-THIN-191222/736
Vendor: thinkphp					
Product: thinkphp					
Affected Version(s): 5.0.24					
Unrestricted Upload of File with Dangerous Type	06-Dec-2022	8.8	Thinkphp 5.1.41 and 5.0.24 has a code logic error which causes file upload getshell. **CVE ID : CVE-2022-44289**	N/A	A-THI-THIN-191222/737
Affected Version(s): 5.1.41					
Unrestricted Upload of File with Dangerous Type	06-Dec-2022	8.8	Thinkphp 5.1.41 and 5.0.24 has a code logic error which causes file upload getshell. **CVE ID : CVE-2022-44289**	N/A	A-THI-THIN-191222/738
Vendor: Tibco					
Product: nimbus					
Affected Version(s): 10.5.0					
URL Redirection to	06-Dec-2022	9.3	The Web Client component of TIBCO Software Inc.'s TIBCO	https://www.tibco.com/ser	A-TIB-NIMB-191222/739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Site ('Open Redirect')			Nimbus contains an easily exploitable vulnerability that allows an unauthenticated attacker with network access to exploit an open redirect on the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO Nimbus: version 10.5.0. **CVE ID : CVE-2022-41559**	vices/support/advisories	
N/A	06-Dec-2022	6.5	The Statement Set Upload via the Web Client component of TIBCO Software Inc.'s TIBCO Nimbus contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute a Denial of Service Attack on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Nimbus: version 10.5.0. **CVE ID : CVE-2022-41560**	https://www.tibco.com/services/support/advisories	A-TIB-NIMB-191222/740
Vendor: tiny					
Product: tinymce					
Affected Version(s): * Up to (excluding) 5.10.7					
Improper Neutralization of Input	08-Dec-2022	6.1	tinymce is an open source rich text editor. A cross-site scripting (XSS) vulnerability was	https://github.com/tinymce/tinymce/commit/6923d8	A-TIN-TINY-191222/741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			discovered in the alert and confirm dialogs when these dialogs were provided with malicious HTML content. This can occur in plugins that use the alert or confirm dialogs, such as in the `image` plugin, which presents these dialogs when certain errors occur. The vulnerability allowed arbitrary JavaScript execution when an alert presented in the TinyMCE UI for the current user. This vulnerability has been patched in TinyMCE 5.10.7 and TinyMCE 6.3.1 by ensuring HTML sanitization was still performed after unwrapping invalid elements. Users are advised to upgrade to either 5.10.7 or 6.3.1. Users unable to upgrade may ensure the the `images_upload_handler` returns a valid value as per the images_upload_handler documentation. **CVE ID : CVE-2022-23494**	5eba6de3e08ebc9c5a387b5abdaa21150e, https://www.tiny.cloud/docs/tinymce/6/file-image-upload/#images_upload_handler, https://www.tiny.cloud/docs/release-notes/release-notes5107/#securityfixes	
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.3.1					
Improper Neutralization of Input During Web Page	08-Dec-2022	6.1	tinymce is an open source rich text editor. A cross-site scripting (XSS) vulnerability was discovered in the alert and confirm dialogs	https://github.com/tinymce/tinymce/commit/6923d85eba6de3e08ebc9c5a387b	A-TIN-TINY-191222/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			when these dialogs were provided with malicious HTML content. This can occur in plugins that use the alert or confirm dialogs, such as in the `image` plugin, which presents these dialogs when certain errors occur. The vulnerability allowed arbitrary JavaScript execution when an alert presented in the TinyMCE UI for the current user. This vulnerability has been patched in TinyMCE 5.10.7 and TinyMCE 6.3.1 by ensuring HTML sanitization was still performed after unwrapping invalid elements. Users are advised to upgrade to either 5.10.7 or 6.3.1. Users unable to upgrade may ensure the the `images_upload_handler` returns a valid value as per the images_upload_handler documentation. **CVE ID : CVE-2022-23494**	5abdaa21150e, https://www.tiny.cloud/docs/tinymce/6/file-image-upload/#images_upload_handler, https://www.tiny.cloud/docs/release-notes/release-notes5107/#securityfixes	
Vendor: traefik					
Product: traefik					
Affected Version(s): * Up to (excluding) 2.9.6					
Insertion of Sensitive Information into Log File	08-Dec-2022	6.5	Traefik is an open source HTTP reverse proxy and load balancer. Versions prior to 2.9.6 are subject to a potential	https://github.com/traefik/traefik/pull/9574, https://githu	A-TRA-TRAE-191222/743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in Traefik displaying the Authorization header in its debug logs. In certain cases, if the log level is set to DEBUG, credentials provided using the Authorization header are displayed in the debug logs. Attackers must have access to a users logging system in order for credentials to be stolen. This issue has been addressed in version 2.9.6. Users are advised to upgrade. Users unable to upgrade may set the log level to `INFO`, `WARN`, or `ERROR`. **CVE ID : CVE-2022-23469**	b.com/traefik/traefik/security/advisories/GHSA-h2ph-vhm7-g4hp	
Improper Certificate Validation	08-Dec-2022	6.5	Traefik is an open source HTTP reverse proxy and load balancer. In affected versions there is a potential vulnerability in Traefik managing TLS connections. A router configured with a not well-formatted TLSOption is exposed with an empty TLSOption. For instance, a route secured using an mTLS connection set with a wrong CA file is exposed without verifying the client certificates. Users are advised to upgrade to version 2.9.6. Users unable to upgrade should	https://github.com/traefik/traefik/security/advisories/GHSA-468w-8x39-gj5v, https://doc.traefik.io/traefik/v2.9/https/tls/#tls-options, https://github.com/traefik/traefik/commit/7e3fe48b80083b41e9ff82a474a36484cabc701a	A-TRA-TRAE-191222/744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check their logs to detect the error messages and fix your TLS options. **CVE ID : CVE-2022-46153**		
Vendor: Trendmicro					
Product: apex_one					
Affected Version(s): -					
N/A	12-Dec-2022	7.1	An arbitrary file deletion vulnerability in the Damage Cleanup Engine component of Trend Micro Apex One and Trend Micro Apex One as a Service could allow a local attacker to escalate privileges and delete files on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-45797**	https://success.trendmicro.com/solution/000291830	A-TRE-APEX-191222/745
Affected Version(s): * Up to (excluding) 14.0.11789					
Out-of-bounds Write	12-Dec-2022	7.8	An out-of-bounds access vulnerability in the Unauthorized Change Prevention service of Trend Micro Apex One and Apex One as a Service could allow a local attacker to elevate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target	https://success.trendmicro.com/solution/000291770	A-TRE-APEX-191222/746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system in order to exploit this vulnerability. **CVE ID : CVE-2022-44649**		
Out-of-bounds Write	12-Dec-2022	7.8	A memory corruption vulnerability in the Unauthorized Change Prevention service of Trend Micro Apex One and Apex One as a Service could allow a local attacker to elevate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-44650**	https://success.trendmicro.com/solution/000291770	A-TRE-APEX-191222/747
Improper Handling of Exceptional Conditions	12-Dec-2022	7.8	An improper handling of exceptional conditions vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-44652**	https://success.trendmicro.com/solution/000291770	A-TRE-APEX-191222/748
Improper Limitation of a	12-Dec-2022	7.8	A security agent directory traversal vulnerability in Trend	https://success.trendmicro.	A-TRE-APEX-191222/749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			Micro Apex One and Apex One as a Service could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-44653**	com/solution /000291770	
N/A	12-Dec-2022	7.5	Affected builds of Trend Micro Apex One and Apex One as a Service contain a monitor engine component that is complied without the /SAFESEH memory protection mechanism which helps to monitor for malicious payloads. The affected component's memory protection mechanism has been updated to enhance product security. **CVE ID : CVE-2022-44654**	https://success.trendmicro.com/solution /000291770	A-TRE-APEX-191222/750
Time-of-check Time-of-use (TOCTOU) Race Condition	12-Dec-2022	7	A Time-of-Check Time-Of-Use vulnerability in the Trend Micro Apex One and Apex One as a Service agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-	https://success.trendmicro.com/solution /000291770	A-TRE-APEX-191222/751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-44651**		
Out-of-bounds Read	12-Dec-2022	5.5	An Out-of-bounds read vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to disclose sensitive information on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is similar to, but not the same as CVE-2022-44648. **CVE ID : CVE-2022-44647**	https://success.trendmicro.com/solution/000291770	A-TRE-APEX-191222/752
Out-of-bounds Read	12-Dec-2022	5.5	An Out-of-bounds read vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to disclose sensitive information on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is similar to, but not the same as CVE-2022-44647.	https://success.trendmicro.com/solution/000291770	A-TRE-APEX-191222/753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-44648		
Affected Version(s): 2019					
Out-of-bounds Write	12-Dec-2022	7.8	An out-of-bounds access vulnerability in the Unauthorized Change Prevention service of Trend Micro Apex One and Apex One as a Service could allow a local attacker to elevate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-44649**	https://success.trendmicro.com/solution/000291770	A-TRE-APEX-191222/754
Out-of-bounds Write	12-Dec-2022	7.8	A memory corruption vulnerability in the Unauthorized Change Prevention service of Trend Micro Apex One and Apex One as a Service could allow a local attacker to elevate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-44650**	https://success.trendmicro.com/solution/000291770	A-TRE-APEX-191222/755
Improper Handling of	12-Dec-2022	7.8	An improper handling of exceptional conditions vulnerability in Trend	https://success.trendmicro.	A-TRE-APEX-191222/756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			Micro Apex One and Apex One as a Service could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-44652**	com/solution/000291770	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Dec-2022	7.8	A security agent directory traversal vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-44653**	https://success.trendmicro.com/solution/000291770	A-TRE-APEX-191222/757
N/A	12-Dec-2022	7.5	Affected builds of Trend Micro Apex One and Apex One as a Service contain a monitor engine component that is complied without the /SAFESEH memory protection mechanism which helps to monitor for malicious payloads. The affected component's memory	https://success.trendmicro.com/solution/000291770	A-TRE-APEX-191222/758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protection mechanism has been updated to enhance product security. **CVE ID : CVE-2022-44654**		
N/A	12-Dec-2022	7.1	An arbitrary file deletion vulnerability in the Damage Cleanup Engine component of Trend Micro Apex One and Trend Micro Apex One as a Service could allow a local attacker to escalate privileges and delete files on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-45797**	https://success.trendmicro.com/solution/000291830	A-TRE-APEX-191222/759
Time-of-check Time-of-use (TOCTOU) Race Condition	12-Dec-2022	7	A Time-of-Check Time-Of-Use vulnerability in the Trend Micro Apex One and Apex One as a Service agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-44651**	https://success.trendmicro.com/solution/000291770	A-TRE-APEX-191222/760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	12-Dec-2022	5.5	An Out-of-bounds read vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to disclose sensitive information on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is similar to, but not the same as CVE-2022-44648. **CVE ID : CVE-2022-44647**	https://success.trendmicro.com/solution/000291770	A-TRE-APEX-191222/761
Out-of-bounds Read	12-Dec-2022	5.5	An Out-of-bounds read vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to disclose sensitive information on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is similar to, but not the same as CVE-2022-44647. **CVE ID : CVE-2022-44648**	https://success.trendmicro.com/solution/000291770	A-TRE-APEX-191222/762
Vendor: typora					
Product: typora					
Affected Version(s): * Up to (excluding) 1.4.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-2022	6.1	Typora versions prior to 1.4.4 fails to properly neutralize JavaScript code, which may result in executing JavaScript code contained in the file when opening a file with the affected product. **CVE ID : CVE-2022-43668**	https://typora.io/releases/all	A-TYP-TYPO-191222/763
Vendor: user_registration_\&_user_management_system_project					
Product: user_registration_\&_user_management_system					
Affected Version(s): 3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	5.4	Phpgurukul User Registration & User Management System v3.0 was discovered to contain multiple stored cross-site scripting (XSS) vulnerabilities via the firstname and lastname parameters of the registration form & login pages. **CVE ID : CVE-2022-43097**	N/A	A-USE-USER-191222/764
Vendor: Veeam					
Product: veeam_backup_for_google_cloud					
Affected Version(s): 1.0					
Improper Authentication	05-Dec-2022	9.8	Improper authentication in Veeam Backup for Google Cloud v1.0 and v3.0 allows attackers to bypass authentication mechanisms. **CVE ID : CVE-2022-43549**	https://www.veeam.com/kb4374	A-VEE-VEEA-191222/765
Affected Version(s): 3.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	05-Dec-2022	9.8	Improper authentication in Veeam Backup for Google Cloud v1.0 and v3.0 allows attackers to bypass authentication mechanisms. **CVE ID : CVE-2022-43549**	https://www.veeam.com/kb4374	A-VEE-VEEA-191222/766
Vendor: Veritas					
Product: access_appliance					
Affected Version(s): * Up to (including) 8.0.100					
N/A	04-Dec-2022	9.8	An issue was discovered in Veritas NetBackup Flex Scale through 3.0 and Access Appliance through 8.0.100. Unauthenticated remote command execution can occur via the management portal. **CVE ID : CVE-2022-46414**	https://www.veritas.com/content/support/en_US/security/VTS22-019#issue1	A-VER-ACCE-191222/767
Use of Hard-coded Credentials	04-Dec-2022	8.8	An issue was discovered in Veritas NetBackup Flex Scale through 3.0 and Access Appliance through 8.0.100. A default password is persisted after installation and may be discovered and used to escalate privileges. **CVE ID : CVE-2022-46411**	https://www.veritas.com/content/support/en_US/security/VTS22-019#issue3	A-VER-ACCE-191222/768
N/A	04-Dec-2022	8.8	An issue was discovered in Veritas NetBackup Flex Scale through 3.0 and Access Appliance through 8.0.100. Authenticated remote command execution can	https://www.veritas.com/content/support/en_US/security/VTS22-019#issue2	A-VER-ACCE-191222/769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			occur via the management portal. **CVE ID : CVE-2022-46413**		
Product: netbackup_flex_scale_appliance					
Affected Version(s): * Up to (including) 3.0					
N/A	04-Dec-2022	9.8	An issue was discovered in Veritas NetBackup Flex Scale through 3.0 and Access Appliance through 8.0.100. Unauthenticated remote command execution can occur via the management portal. **CVE ID : CVE-2022-46414**	https://www.veritas.com/content/support/en_US/security/VTS22-019#issue1	A-VER-NETB-191222/770
Improper Privilege Management	04-Dec-2022	8.8	An issue was discovered in Veritas NetBackup Flex Scale through 3.0. An attacker with non-root privileges may escalate privileges to root by using specific commands. **CVE ID : CVE-2022-46410**	https://www.veritas.com/content/support/en_US/security/VTS22-019#issue5	A-VER-NETB-191222/771
Use of Hard-coded Credentials	04-Dec-2022	8.8	An issue was discovered in Veritas NetBackup Flex Scale through 3.0 and Access Appliance through 8.0.100. A default password is persisted after installation and may be discovered and used to escalate privileges. **CVE ID : CVE-2022-46411**	https://www.veritas.com/content/support/en_US/security/VTS22-019#issue3	A-VER-NETB-191222/772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Dec-2022	8.8	An issue was discovered in Veritas NetBackup Flex Scale through 3.0. A non-privileged user may escape a restricted shell and execute privileged commands. **CVE ID : CVE-2022-46412**	https://www.veritas.com/content/support/en_US/security/VTS22-019#issue4	A-VER-NETB-191222/773
N/A	04-Dec-2022	8.8	An issue was discovered in Veritas NetBackup Flex Scale through 3.0 and Access Appliance through 8.0.100. Authenticated remote command execution can occur via the management portal. **CVE ID : CVE-2022-46413**	https://www.veritas.com/content/support/en_US/security/VTS22-019#issue2	A-VER-NETB-191222/774
Vendor: Videolan					
Product: vlc_media_player					
Affected Version(s): * Up to (including) 3.0.17.4					
Integer Overflow or Wraparound	06-Dec-2022	7.8	An integer overflow in the VNC module in VideoLAN VLC Media Player through 3.0.17.4 allows attackers, by tricking a user into opening a crafted playlist or connecting to a rogue VNC server, to crash VLC or execute code under some conditions. **CVE ID : CVE-2022-41325**	https://www.videolan.org/security/sb-vlc3018.html, https://www.synacktiv.com/sites/default/files/2022-11/vlc_vnc_int_overflow-CVE-2022-41325.pdf	A-VID-VLC_-191222/775
Vendor: VIM					
Product: vim					
Affected Version(s): * Up to (excluding) 9.0.0742					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	03-Dec-2022	9.8	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0742. **CVE ID : CVE-2022-3491**	https://huntr.dev/bounties/6e6e05c2-2cf7-4aa5-a817-a62007bf92cb, https://github.com/vim/vim/commit/3558afe9e9e904cabb8475392d859f2d2fc21041	A-VIM-VIM-191222/776
Affected Version(s): * Up to (excluding) 9.0.0765					
Out-of-bounds Write	02-Dec-2022	9.8	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0765. **CVE ID : CVE-2022-3520**	https://github.com/vim/vim/commit/36343ae0fb7247e060abfd35fb8e4337b33abb4b, https://huntr.dev/bounties/c1db3b70-f4fe-481f-8a24-0b1449c94246	A-VIM-VIM-191222/777
Affected Version(s): * Up to (excluding) 9.0.0789					
Use After Free	02-Dec-2022	7.8	Use After Free in GitHub repository vim/vim prior to 9.0.0789. **CVE ID : CVE-2022-3591**	https://github.com/vim/vim/commit/8f3c3c6cd044e3b5bf08dbfa3b3f04bb3f711bad, https://huntr.dev/bounties/a5a998c2-4b07-47a7-91be-	A-VIM-VIM-191222/778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				dbc1886b3921	
Affected Version(s): * Up to (excluding) 9.0.0804					
Incorrect Comparison	05-Dec-2022	5.5	Floating Point Comparison with Incorrect Operator in GitHub repository vim/vim prior to 9.0.0804. **CVE ID : CVE-2022-4293**	https://huntr.dev/bounties/385a835f-6e33-4d00-acce-ac99f3939143, https://github.com/vim/vim/commit/cdef1cefa2a440911c727558562f83ed9b00e16b	A-VIM-VIM-191222/779
Affected Version(s): * Up to (excluding) 9.0.0882					
Use After Free	05-Dec-2022	7.8	Use After Free in GitHub repository vim/vim prior to 9.0.0882. **CVE ID : CVE-2022-4292**	https://huntr.dev/bounties/da3d4c47-e57a-451e-993d-9df0ed31f57b, https://github.com/vim/vim/commit/c3d27ada14acd02db357f2d16347acc22cb17e93	A-VIM-VIM-191222/780
Vendor: warehouse_management_system_project					
Product: warehouse_management_system					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	03-Dec-2022	9.8	A vulnerability, which was classified as critical, has been found in FeMiner wms. Affected by this issue is some unknown functionality of	N/A	A-WAR-WARE-191222/781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the file /product/savenewproduct.php?flag=1. The manipulation of the argument upfile leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-214760. **CVE ID : CVE-2022-4272**		
Vendor: webtareas_project					
Product: webtareas					
Affected Version(s): 2.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-2022	9.8	webTareas 2.4p5 was discovered to contain a SQL injection vulnerability via the id parameter in deleteapprovalstages.php. **CVE ID : CVE-2022-44290**	N/A	A-WEB-WEBT-191222/782
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-2022	9.8	webTareas 2.4p5 was discovered to contain a SQL injection vulnerability via the id parameter in phasesets.php. **CVE ID : CVE-2022-44291**	N/A	A-WEB-WEBT-191222/783
Improper Neutralization of Input	02-Dec-2022	5.4	webtareas 2.4p5 was discovered to contain a cross-site scripting (XSS) vulnerability in the	N/A	A-WEB-WEBT-191222/784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			component /linkedcontent/listfiles.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field after clicking "Add". **CVE ID : CVE-2022-44953**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	5.4	webtareas 2.4p5 was discovered to contain a cross-site scripting (XSS) vulnerability in the component /contacts/listcontacts.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Last Name field after clicking "Add". **CVE ID : CVE-2022-44954**	N/A	A-WEB-WEBT-191222/785
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	5.4	webtareas 2.4p5 was discovered to contain a cross-site scripting (XSS) vulnerability in the Chat function. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Messages field. **CVE ID : CVE-2022-44955**	N/A	A-WEB-WEBT-191222/786
Improper Neutralization of	02-Dec-2022	5.4	webtareas 2.4p5 was discovered to contain a cross-site scripting (XSS)	N/A	A-WEB-WEBT-191222/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			vulnerability in the component /projects/listprojects.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2022-44956**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	5.4	webtareas 2.4p5 was discovered to contain a cross-site scripting (XSS) vulnerability in the component /clients/listclients.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2022-44957**	N/A	A-WEB-WEBT-191222/788
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	5.4	webtareas 2.4p5 was discovered to contain a cross-site scripting (XSS) vulnerability in the component /meetings/listmeetings.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2022-44959**	N/A	A-WEB-WEBT-191222/789
Improper Neutralization of	02-Dec-2022	5.4	webtareas 2.4p5 was discovered to contain a cross-site scripting (XSS)	N/A	A-WEB-WEBT-191222/790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			vulnerability in the component /general/search.php?searchtype=simple. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Search field. **CVE ID : CVE-2022-44960**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	5.4	webtareas 2.4p5 was discovered to contain a cross-site scripting (XSS) vulnerability in the component /forums/editforum.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2022-44961**	N/A	A-WEB-WEBT-191222/791
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Dec-2022	5.4	webtareas 2.4p5 was discovered to contain a cross-site scripting (XSS) vulnerability in the component /calendar/viewcalendar.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Subject field. **CVE ID : CVE-2022-44962**	N/A	A-WEB-WEBT-191222/792
Vendor: wedevs					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: dokan					
Affected Version(s): * Up to (excluding) 3.7.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Dec-2022	9.8	The Dokan WordPress plugin before 3.7.6 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-2022-3915**	N/A	A-WED-DOKA-191222/793
Vendor: whitestudio					
Product: easy_form_builder					
Affected Version(s): * Up to (excluding) 3.4.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2022	4.8	The Easy Form Builder WordPress plugin before 3.4.0 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-2022-3906**	N/A	A-WHI-EASY-191222/794
Vendor: Wireshark					
Product: wireshark					
Affected Version(s): From (including) 3.6.0 Up to (including) 3.6.8					
Improper Neutralization of Special Elements in Output	09-Dec-2022	7.5	Crash in the USB HID protocol dissector in Wireshark 3.6.0 to 3.6.8 allows denial of service via packet injection or	https://www.wireshark.org/security/wnpa-sec-2022-08.html, https://gitlab.	A-WIR-WIRE-191222/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Used by a Downstream Component ('Injection')			crafted capture file on Windows **CVE ID : CVE-2022-3724**	com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3724.json	
Vendor: Wordpress					
Product: wordpress					
Affected Version(s): * Up to (excluding) 6.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	6.1	Cross-site scripting vulnerability in WordPress versions prior to 6.0.3 allows a remote unauthenticated attacker to inject an arbitrary script . **CVE ID : CVE-2022-43497**	https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/	A-WOR-WORD-191222/796
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	6.1	Cross-site scripting vulnerability in WordPress versions prior to 6.0.3 allows a remote unauthenticated attacker to inject an arbitrary script . **CVE ID : CVE-2022-43500**	https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/	A-WOR-WORD-191222/797
Improper Authentication	05-Dec-2022	5.3	Improper authentication vulnerability in WordPress versions prior to 6.0.3 allows a remote unauthenticated attacker to obtain the email address of the user who posted a blog using the WordPress Post by Email Feature. **CVE ID : CVE-2022-43504**	https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/, https://wordpress.org/download/	A-WOR-WORD-191222/798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: wordpress_popular_posts_project					
Product: wordpress_popular_posts					
Affected Version(s): * Up to (including) 6.0.5					
Improper Initialization	07-Dec-2022	7.5	External initialization of trusted variables or data stores vulnerability exists in WordPress Popular Posts 6.0.5 and earlier, therefore the vulnerable product accepts untrusted external inputs to update certain internal variables. As a result, the number of views for an article may be manipulated through a crafted input. **CVE ID : CVE-2022-43468**	N/A	A-WOR-WORD-191222/799
Vendor: Wp-ecommerce					
Product: easy_wp_smtp					
Affected Version(s): * Up to (including) 1.5.1					
Improper Control of Generation of Code ('Code Injection')	06-Dec-2022	8.8	Auth. Remote Code Execution vulnerability in Easy WP SMTP plugin <= 1.5.1 on WordPress. **CVE ID : CVE-2022-42699**	N/A	A-WP--EASY-191222/800
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Dec-2022	8.1	Auth. Path Traversal vulnerability in Easy WP SMTP plugin <= 1.5.1 at WordPress. **CVE ID : CVE-2022-45829**	N/A	A-WP--EASY-191222/801
Improper Limitation	06-Dec-2022	6.5	Auth. Path Traversal vulnerability in Easy WP	N/A	A-WP--EASY-191222/802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			SMTP plugin <= 1.5.1 on WordPress. **CVE ID : CVE-2022-45833**		
Vendor: wp-oauth					
Product: wp_oauth_server					
Affected Version(s): * Up to (excluding) 3.4.2					
Cross-Site Request Forgery (CSRF)	05-Dec-2022	6.5	The WP OAuth Server (OAuth Authentication) WordPress plugin before 3.4.2 does not have CSRF check when regenerating secrets, which could allow attackers to make logged in admins regenerate the secret of an arbitrary client given they know the client ID **CVE ID : CVE-2022-3926**	N/A	A-WP--WP_O-191222/803
Affected Version(s): * Up to (excluding) 4.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	The WP OAuth Server (OAuth Authentication) WordPress plugin before 4.2.2 does not sanitize and escape Client IDs, 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-2022-3892**	N/A	A-WP--WP_O-191222/804
Vendor: wpdevart					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: booking_calendar					
Affected Version(s): * Up to (excluding) 3.2.2					
Unrestricted Upload of File with Dangerous Type	12-Dec-2022	9.8	The Booking calendar, Appointment Booking System WordPress plugin before 3.2.2 does not validate uploaded files, which could allow unauthenticated users to upload arbitrary files, such as PHP and achieve RCE **CVE ID : CVE-2022-3982**	N/A	A-WPD-BOOK-191222/805
Vendor: wpeverest					
Product: user_registration					
Affected Version(s): * Up to (excluding) 2.2.4.1					
Unrestricted Upload of File with Dangerous Type	12-Dec-2022	7.5	The User Registration WordPress plugin before 2.2.4.1 does not properly restrict the files to be uploaded via an AJAX action available to both unauthenticated and authenticated users, which could allow unauthenticated users to upload PHP files for example. **CVE ID : CVE-2022-3912**	N/A	A-WPE-USER-191222/806
Vendor: wpmanage					
Product: uji_countdown					
Affected Version(s): * Up to (including) 2.2					
Improper Neutralization of Input During Web Page	05-Dec-2022	4.8	The Uji Countdown WordPress plugin through 2.2 does not sanitise and escape some of its settings, which could allow high	N/A	A-WPM-UJI_-191222/807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			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-2022-3837**		
Vendor: wptools_project					
Product: wptools					
Affected Version(s): * Up to (excluding) 3.43					
Cross-Site Request Forgery (CSRF)	12-Dec-2022	5.7	The WP Tools Increase Maximum Limits, Repair, Server PHP Info, Javascript errors, File Permissions, Transients, Error Log WordPress plugin before 3.43 does not have proper authorisation and CSRF in an AJAX action, allowing any authenticated users, such as subscriber to call it and install and activate arbitrary plugins from wordpress.org **CVE ID : CVE-2022-3881**	N/A	A-WPT-WPTO-191222/808
Vendor: wpupper_share_buttons_project					
Product: wpupper_share_buttons					
Affected Version(s): * Up to (including) 3.42					
Improper Neutralization of Input During Web Page Generation	05-Dec-2022	4.8	The WPUpper Share Buttons WordPress plugin through 3.42 does not sanitise and escape some of its settings, which could allow high privilege users such as	N/A	A-WPU-WPUP-191222/809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID : CVE-2022-3838**		
Vendor: wpwax					
Product: directorist					
Affected Version(s): * Up to (excluding) 7.4.2.2					
Authorization Bypass Through User-Controlled Key	12-Dec-2022	6.5	The Directorist WordPress plugin before 7.4.2.2 suffers from an IDOR vulnerability which an attacker can exploit to change the password of arbitrary users instead of his own. **CVE ID : CVE-2022-3930**	N/A	A-WPW-DIRE-191222/810
Vendor: wp_csv_exporter_project					
Product: wp_csv_exporter					
Affected Version(s): * Up to (excluding) 1.3.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Dec-2022	7.2	The WP CSV Exporter WordPress plugin before 1.3.7 does not properly sanitise and escape some parameters before using them in a SQL statement, allowing high privilege users such as admin to perform SQL injection attacks **CVE ID : CVE-2022-3249**	N/A	A-WP_-WP_C-191222/811
Vendor: xjd2020					
Product: fastcms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Dec-2022	8.8	A vulnerability was found in FastCMS. It has been rated as critical. This issue affects some unknown processing of the file /template/edit of the component Template Handler. The manipulation leads to injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-214901 was assigned to this vulnerability. **CVE ID : CVE-2022-4300**	N/A	A-XJD-FAST-191222/812
Vendor: xylusthemes					
Product: wp_smart_import					
Affected Version(s): * Up to (including) 1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Xylus Themes WP Smart Import plugin <= 1.0.2 on WordPress. **CVE ID : CVE-2022-40209**	N/A	A-XYL-WP_S-191222/813
Vendor: yet_another_useragent_analyzer_project					
Product: yet_another_useragent_analyzer					
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.9.0					
Improper Handling of Exceptiona	08-Dec-2022	7.5	Yet Another UserAgent Analyzer (Yauaa) is a java library that tries to parse and analyze the useragent string and	https://github.com/nielsbasjes/yauaa/commit/3017a866e2cff0d308	A-YET-YET_-191222/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			extract as many relevant attributes as possible. Applications using the Client Hints analysis feature introduced with 7.0.0 can crash because the Yauaa library throws an ArrayIndexOutOfBounds Exception. If uncaught the exception will result in a program crash. Applications that do not use this feature are not affected. Users are advised to upgrade to version 7.9.0. Users unable to upgrade may catch and discard any ArrayIndexOutOfBounds Exception thrown by the Yauaa library. **CVE ID : CVE-2022-23496**	f264b66fde4fa79e3beb9e	
Vendor: Yiiframework					
Product: gii					
Affected Version(s): * Up to (including) 2.2.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-2022	5.4	Yii Yii2 Gii through 2.2.4 allows stored XSS by injecting a payload into any field. **CVE ID : CVE-2022-34297**	N/A	A-YII-GII-191222/815
Vendor: yithemes					
Product: yith_woocommerce_gift_cards					
Affected Version(s): * Up to (including) 3.19.0					
Unrestricted Upload of	06-Dec-2022	9.8	Unauth. Arbitrary File Upload vulnerability in	N/A	A-YIT-YITH-191222/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			YITH WooCommerce Gift Cards premium plugin <= 3.19.0 on WordPress. **CVE ID : CVE-2022-45359**		
Vendor: Zabbix					
Product: frontend					
Affected Version(s): 5.0.30					
Incorrect Authorization	05-Dec-2022	9.8	Zabbix Frontend provides a feature that allows admins to maintain the installation and ensure that only certain IP addresses can access it. In this way, any user will not be able to access the Zabbix Frontend while it is being maintained and possible sensitive data will be prevented from being disclosed. An attacker can bypass this protection and access the instance using IP address not listed in the defined range. **CVE ID : CVE-2022-43515**	N/A	A-ZAB-FRON-191222/817
Affected Version(s): 6.0.11					
Incorrect Authorization	05-Dec-2022	9.8	Zabbix Frontend provides a feature that allows admins to maintain the installation and ensure that only certain IP addresses can access it. In this way, any user will not be able to access the Zabbix Frontend while it is being maintained and possible	N/A	A-ZAB-FRON-191222/818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive data will be prevented from being disclosed. An attacker can bypass this protection and access the instance using IP address not listed in the defined range. **CVE ID : CVE-2022-43515**		
Affected Version(s): 6.2.5					
Incorrect Authorization	05-Dec-2022	9.8	Zabbix Frontend provides a feature that allows admins to maintain the installation and ensure that only certain IP addresses can access it. In this way, any user will not be able to access the Zabbix Frontend while it is being maintained and possible sensitive data will be prevented from being disclosed. An attacker can bypass this protection and access the instance using IP address not listed in the defined range. **CVE ID : CVE-2022-43515**	N/A	A-ZAB-FRON-191222/819
Affected Version(s): From (including) 4.0.0 Up to (including) 4.0.44					
Incorrect Authorization	05-Dec-2022	9.8	Zabbix Frontend provides a feature that allows admins to maintain the installation and ensure that only certain IP addresses can access it. In this way, any user will not be able to access the Zabbix	N/A	A-ZAB-FRON-191222/820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Frontend while it is being maintained and possible sensitive data will be prevented from being disclosed. An attacker can bypass this protection and access the instance using IP address not listed in the defined range. **CVE ID : CVE-2022-43515**		
Affected Version(s): From (including) 5.0.0 Up to (including) 5.0.29					
Incorrect Authorization	05-Dec-2022	9.8	Zabbix Frontend provides a feature that allows admins to maintain the installation and ensure that only certain IP addresses can access it. In this way, any user will not be able to access the Zabbix Frontend while it is being maintained and possible sensitive data will be prevented from being disclosed. An attacker can bypass this protection and access the instance using IP address not listed in the defined range. **CVE ID : CVE-2022-43515**	N/A	A-ZAB-FRON-191222/821
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.9					
Incorrect Authorization	05-Dec-2022	9.8	Zabbix Frontend provides a feature that allows admins to maintain the installation and ensure that only certain IP addresses can access it. In this way, any	N/A	A-ZAB-FRON-191222/822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user will not be able to access the Zabbix Frontend while it is being maintained and possible sensitive data will be prevented from being disclosed. An attacker can bypass this protection and access the instance using IP address not listed in the defined range. **CVE ID : CVE-2022-43515**		
Affected Version(s): From (including) 6.2.0 Up to (including) 6.2.4					
Incorrect Authorization	05-Dec-2022	9.8	Zabbix Frontend provides a feature that allows admins to maintain the installation and ensure that only certain IP addresses can access it. In this way, any user will not be able to access the Zabbix Frontend while it is being maintained and possible sensitive data will be prevented from being disclosed. An attacker can bypass this protection and access the instance using IP address not listed in the defined range. **CVE ID : CVE-2022-43515**	N/A	A-ZAB-FRON-191222/823
Product: Zabbix					
Affected Version(s): 6.0.12					
N/A	05-Dec-2022	9.8	A Firewall Rule which allows all incoming TCP connections to all programs from any	https://support.zabbix.com	A-ZAB-ZABB-191222/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			source and to all ports is created in Windows Firewall after Zabbix agent installation (MSI) **CVE ID : CVE-2022-43516**	/browse/ZBX-22002	
Affected Version(s): 6.2.6					
N/A	05-Dec-2022	9.8	A Firewall Rule which allows all incoming TCP connections to all programs from any source and to all ports is created in Windows Firewall after Zabbix agent installation (MSI) **CVE ID : CVE-2022-43516**	https://support.zabbix.com/browse/ZBX-22002	A-ZAB-ZABB-191222/825
Affected Version(s): From (including) 6.0.10 Up to (excluding) 6.0.12					
N/A	05-Dec-2022	9.8	A Firewall Rule which allows all incoming TCP connections to all programs from any source and to all ports is created in Windows Firewall after Zabbix agent installation (MSI) **CVE ID : CVE-2022-43516**	https://support.zabbix.com/browse/ZBX-22002	A-ZAB-ZABB-191222/826
Affected Version(s): From (including) 6.2.0 Up to (excluding) 6.2.6					
N/A	05-Dec-2022	9.8	A Firewall Rule which allows all incoming TCP connections to all programs from any source and to all ports is created in Windows Firewall after Zabbix agent installation (MSI) **CVE ID : CVE-2022-43516**	https://support.zabbix.com/browse/ZBX-22002	A-ZAB-ZABB-191222/827
Vendor: zend-blog-2_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: zend-blog-2					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	10-Dec-2022	6.5	A vulnerability was found in morontt zend-blog-number-2. It has been classified as problematic. Affected is an unknown function of the file application/forms/Comment.php of the component Comment Handler. The manipulation leads to cross-site request forgery. It is possible to launch the attack remotely. The name of the patch is 36b2d4abe20a6245e4f8df7a4b14e130b24d429d. It is recommended to apply a patch to fix this issue. VDB-215250 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4397**	https://github.com/morontt/zend-blog-number-2/commit/36b2d4abe20a6245e4f8df7a4b14e130b24d429d	A-ZEN-ZEND-191222/828
Vendor: Zimbra					
Product: collaboration					
Affected Version(s): 8.8.15					
Unrestricted Upload of File with Dangerous Type	05-Dec-2022	7.2	An issue was discovered in Zimbra Collaboration (ZCS) 8.8.15 and 9.0. Remote code execution can occur through ClientUploader by an authenticated admin user. An authenticated admin user can upload files through the ClientUploader utility,	N/A	A-ZIM-COLL-191222/829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and traverse to any other directory for remote code execution. **CVE ID : CVE-2022-45912**		
Affected Version(s): 9.0.0					
Unrestricted Upload of File with Dangerous Type	05-Dec-2022	7.2	An issue was discovered in Zimbra Collaboration (ZCS) 8.8.15 and 9.0. Remote code execution can occur through ClientUploader by an authenticated admin user. An authenticated admin user can upload files through the ClientUploader utility, and traverse to any other directory for remote code execution. **CVE ID : CVE-2022-45912**	N/A	A-ZIM-COLL-191222/830
Vendor: zkteco					
Product: automatic_data_master_server					
Affected Version(s): * Up to (including) 3.1-164					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-2022	4.8	ZKTeco Xiamen Information Technology ZKBio ECO ADMS <=3.1-164 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2022-44213**	N/A	A-ZKT-AUTO-191222/831
Vendor: zzcms					
Product: zzcms					
Affected Version(s): 2022					
Improper Neutralization of	07-Dec-2022	5.4	An issue was discovered in ZZCMS 2022. There is a cross-site scripting	N/A	A-ZZC-ZZCM-191222/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			(XSS) vulnerability in admin/ad_list.php. **CVE ID : CVE-2022-44361**		
Hardware					
Vendor: Arubanetworks					
Product: 7005					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	8.8	Vulnerabilities in ArubaOS running on 7xxx series controllers exist that allows an attacker to execute arbitrary code during the boot sequence. Successful exploitation could allow an attacker to achieve permanent modification of the underlying operating system. **CVE ID : CVE-2022-37904**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7005-191222/833
N/A	12-Dec-2022	7.5	A vulnerability exists in the ArubaOS bootloader on 7xxx series controllers which can result in a denial of service (DoS) condition on an impacted system. A successful attacker can cause a system hang which can only be resolved via a power cycle of the impacted controller. **CVE ID : CVE-2022-37907**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7005-191222/834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2022	6.5	An authenticated attacker can impact the integrity of the ArubaOS bootloader on 7xxx series controllers. Successful exploitation can compromise the hardware chain of trust on the impacted controller. **CVE ID : CVE-2022-37908**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7005-191222/835
Product: 7008					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	8.8	Vulnerabilities in ArubaOS running on 7xxx series controllers exist that allows an attacker to execute arbitrary code during the boot sequence. Successful exploitation could allow an attacker to achieve permanent modification of the underlying operating system. **CVE ID : CVE-2022-37904**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7008-191222/836
N/A	12-Dec-2022	7.5	A vulnerability exists in the ArubaOS bootloader on 7xxx series controllers which can result in a denial of service (DoS) condition on an impacted system. A successful attacker can cause a system hang which can only be resolved via a power cycle of the impacted controller.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7008-191222/837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37907		
N/A	12-Dec-2022	6.5	An authenticated attacker can impact the integrity of the ArubaOS bootloader on 7xxx series controllers. Successful exploitation can compromise the hardware chain of trust on the impacted controller. **CVE ID : CVE-2022-37908**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7008-191222/838
Product: 7010					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	8.8	Vulnerabilities in ArubaOS running on 7xxx series controllers exist that allows an attacker to execute arbitrary code during the boot sequence. Successful exploitation could allow an attacker to achieve permanent modification of the underlying operating system. **CVE ID : CVE-2022-37904**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7010-191222/839
N/A	12-Dec-2022	7.5	A vulnerability exists in the ArubaOS bootloader on 7xxx series controllers which can result in a denial of service (DoS) condition on an impacted system. A successful attacker can cause a system hang which can only be resolved via a power	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7010-191222/840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cycle of the impacted controller. **CVE ID : CVE-2022-37907**		
N/A	12-Dec-2022	6.5	An authenticated attacker can impact the integrity of the ArubaOS bootloader on 7xxx series controllers. Successful exploitation can compromise the hardware chain of trust on the impacted controller. **CVE ID : CVE-2022-37908**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7010-191222/841
Product: 7024					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	8.8	Vulnerabilities in ArubaOS running on 7xxx series controllers exist that allows an attacker to execute arbitrary code during the boot sequence. Successful exploitation could allow an attacker to achieve permanent modification of the underlying operating system. **CVE ID : CVE-2022-37904**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7024-191222/842
N/A	12-Dec-2022	7.5	A vulnerability exists in the ArubaOS bootloader on 7xxx series controllers which can result in a denial of service (DoS) condition on an impacted system. A successful attacker can	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7024-191222/843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a system hang which can only be resolved via a power cycle of the impacted controller. **CVE ID : CVE-2022-37907**		
N/A	12-Dec-2022	6.5	An authenticated attacker can impact the integrity of the ArubaOS bootloader on 7xxx series controllers. Successful exploitation can compromise the hardware chain of trust on the impacted controller. **CVE ID : CVE-2022-37908**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7024-191222/844
Product: 7030					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	8.8	Vulnerabilities in ArubaOS running on 7xxx series controllers exist that allows an attacker to execute arbitrary code during the boot sequence. Successful exploitation could allow an attacker to achieve permanent modification of the underlying operating system. **CVE ID : CVE-2022-37904**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7030-191222/845
N/A	12-Dec-2022	7.5	A vulnerability exists in the ArubaOS bootloader on 7xxx series controllers which can result in a denial of	https://www.arubanetworks.com/assets/alert/ARUBA-	H-ARU-7030-191222/846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition on an impacted system. A successful attacker can cause a system hang which can only be resolved via a power cycle of the impacted controller. **CVE ID : CVE-2022-37907**	PSA-2022-016.txt	
N/A	12-Dec-2022	6.5	An authenticated attacker can impact the integrity of the ArubaOS bootloader on 7xxx series controllers. Successful exploitation can compromise the hardware chain of trust on the impacted controller. **CVE ID : CVE-2022-37908**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7030-191222/847
Product: 7205					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	8.8	Vulnerabilities in ArubaOS running on 7xxx series controllers exist that allows an attacker to execute arbitrary code during the boot sequence. Successful exploitation could allow an attacker to achieve permanent modification of the underlying operating system. **CVE ID : CVE-2022-37904**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7205-191222/848
N/A	12-Dec-2022	7.5	A vulnerability exists in the ArubaOS bootloader	https://www.arubanetwork	H-ARU-7205-191222/849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on 7xxx series controllers which can result in a denial of service (DoS) condition on an impacted system. A successful attacker can cause a system hang which can only be resolved via a power cycle of the impacted controller. **CVE ID : CVE-2022-37907**	s.com/assets/alert/ARUBA-PSA-2022-016.txt	
N/A	12-Dec-2022	6.5	An authenticated attacker can impact the integrity of the ArubaOS bootloader on 7xxx series controllers. Successful exploitation can compromise the hardware chain of trust on the impacted controller. **CVE ID : CVE-2022-37908**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7205-191222/850
Product: 7210					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	8.8	Vulnerabilities in ArubaOS running on 7xxx series controllers exist that allows an attacker to execute arbitrary code during the boot sequence. Successful exploitation could allow an attacker to achieve permanent modification of the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7210-191222/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37904		
N/A	12-Dec-2022	7.5	A vulnerability exists in the ArubaOS bootloader on 7xxx series controllers which can result in a denial of service (DoS) condition on an impacted system. A successful attacker can cause a system hang which can only be resolved via a power cycle of the impacted controller. **CVE ID : CVE-2022-37907**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7210-191222/852
N/A	12-Dec-2022	6.5	An authenticated attacker can impact the integrity of the ArubaOS bootloader on 7xxx series controllers. Successful exploitation can compromise the hardware chain of trust on the impacted controller. **CVE ID : CVE-2022-37908**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7210-191222/853
Product: 7220					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	8.8	Vulnerabilities in ArubaOS running on 7xxx series controllers exist that allows an attacker to execute arbitrary code during the boot sequence. Successful exploitation could allow an attacker to achieve permanent modification of the	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7220-191222/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system. **CVE ID : CVE-2022-37904**		
N/A	12-Dec-2022	7.5	A vulnerability exists in the ArubaOS bootloader on 7xxx series controllers which can result in a denial of service (DoS) condition on an impacted system. A successful attacker can cause a system hang which can only be resolved via a power cycle of the impacted controller. **CVE ID : CVE-2022-37907**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7220-191222/855
N/A	12-Dec-2022	6.5	An authenticated attacker can impact the integrity of the ArubaOS bootloader on 7xxx series controllers. Successful exploitation can compromise the hardware chain of trust on the impacted controller. **CVE ID : CVE-2022-37908**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7220-191222/856
Product: 7240xm					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	8.8	Vulnerabilities in ArubaOS running on 7xxx series controllers exist that allows an attacker to execute arbitrary code during the boot sequence. Successful exploitation	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7240-191222/857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an attacker to achieve permanent modification of the underlying operating system. **CVE ID : CVE-2022-37904**		
N/A	12-Dec-2022	7.5	A vulnerability exists in the ArubaOS bootloader on 7xxx series controllers which can result in a denial of service (DoS) condition on an impacted system. A successful attacker can cause a system hang which can only be resolved via a power cycle of the impacted controller. **CVE ID : CVE-2022-37907**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7240-191222/858
N/A	12-Dec-2022	6.5	An authenticated attacker can impact the integrity of the ArubaOS bootloader on 7xxx series controllers. Successful exploitation can compromise the hardware chain of trust on the impacted controller. **CVE ID : CVE-2022-37908**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7240-191222/859
Product: 7280					
Affected Version(s): -					
Improper Control of Generation of Code	12-Dec-2022	8.8	Vulnerabilities in ArubaOS running on 7xxx series controllers exist that allows an attacker to execute	https://www.arubanetworks.com/assets/alert/ARUBA-	H-ARU-7280-191222/860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			arbitrary code during the boot sequence. Successful exploitation could allow an attacker to achieve permanent modification of the underlying operating system. **CVE ID : CVE-2022-37904**	PSA-2022-016.txt	
N/A	12-Dec-2022	7.5	A vulnerability exists in the ArubaOS bootloader on 7xxx series controllers which can result in a denial of service (DoS) condition on an impacted system. A successful attacker can cause a system hang which can only be resolved via a power cycle of the impacted controller. **CVE ID : CVE-2022-37907**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7280-191222/861
N/A	12-Dec-2022	6.5	An authenticated attacker can impact the integrity of the ArubaOS bootloader on 7xxx series controllers. Successful exploitation can compromise the hardware chain of trust on the impacted controller. **CVE ID : CVE-2022-37908**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	H-ARU-7280-191222/862
Vendor: Asus					
Product: nas-m25					
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')	01-Dec-2022	9.8	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Asus NAS-M25 allows an unauthenticated attacker to inject arbitrary OS commands via unsanitized cookie values.This issue affects NAS-M25: through 1.0.1.7. **CVE ID : CVE-2022-4221**	N/A	H-ASU-NAS--191222/863
Vendor: BD					
Product: bodyguard_121_twins					
Affected Version(s): -					
Improper Authentication	05-Dec-2022	5.3	The BD BodyGuard™ infusion pumps specified allow for access through the RS-232 (serial) port interface. If exploited, threat actors with physical access, specialized equipment and knowledge may be able to configure or disable the pump. No electronic protected health information (ePHI), protected health information (PHI) or personally identifiable information (PII) is stored in the pump. **CVE ID : CVE-2022-43557**	https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/bd-bodyguard-pumps-rs-232-interface-vulnerability	H-BD-BODY-191222/864
Product: bodyguard_323_colorvision					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	05-Dec-2022	5.3	The BD BodyGuard™ infusion pumps specified allow for access through the RS-232 (serial) port interface. If exploited, threat actors with physical access, specialized equipment and knowledge may be able to configure or disable the pump. No electronic protected health information (ePHI), protected health information (PHI) or personally identifiable information (PII) is stored in the pump. **CVE ID : CVE-2022-43557**	https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/bd-bodyguard-pumps-rs-232-interface-vulnerability	H-BD-BODY-191222/865
Product: bodyguard_999-603					
Affected Version(s): -					
Improper Authentication	05-Dec-2022	5.3	The BD BodyGuard™ infusion pumps specified allow for access through the RS-232 (serial) port interface. If exploited, threat actors with physical access, specialized equipment and knowledge may be able to configure or disable the pump. No electronic protected health information (ePHI), protected health information (PHI) or personally identifiable information (PII) is stored in the pump. **CVE ID : CVE-2022-43557**	https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/bd-bodyguard-pumps-rs-232-interface-vulnerability	H-BD-BODY-191222/866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: bodyguard_duo_999-903					
Affected Version(s): -					
Improper Authentication	05-Dec-2022	5.3	The BD BodyGuard™ infusion pumps specified allow for access through the RS-232 (serial) port interface. If exploited, threat actors with physical access, specialized equipment and knowledge may be able to configure or disable the pump. No electronic protected health information (ePHI), protected health information (PHI) or personally identifiable information (PII) is stored in the pump. **CVE ID : CVE-2022-43557**	https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/bd-bodyguard-pumps-rs-232-interface-vulnerability	H-BD-BODY-191222/867
Product: bodyguard_epidural_999-683					
Affected Version(s): -					
Improper Authentication	05-Dec-2022	5.3	The BD BodyGuard™ infusion pumps specified allow for access through the RS-232 (serial) port interface. If exploited, threat actors with physical access, specialized equipment and knowledge may be able to configure or disable the pump. No electronic protected health information (ePHI), protected health information (PHI) or personally identifiable information (PII) is stored in the pump.	https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/bd-bodyguard-pumps-rs-232-interface-vulnerability	H-BD-BODY-191222/868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43557		
Product: bodyguard_pain_manager_999-803					
Affected Version(s): -					
Improper Authentication	05-Dec-2022	5.3	The BD BodyGuard™ infusion pumps specified allow for access through the RS-232 (serial) port interface. If exploited, threat actors with physical access, specialized equipment and knowledge may be able to configure or disable the pump. No electronic protected health information (ePHI), protected health information (PHI) or personally identifiable information (PII) is stored in the pump. **CVE ID : CVE-2022-43557**	https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/bd-bodyguard-pumps-rs-232-interface-vulnerability	H-BD-BODY-191222/869
Product: bodyguard_t_999-103					
Affected Version(s): -					
Improper Authentication	05-Dec-2022	5.3	The BD BodyGuard™ infusion pumps specified allow for access through the RS-232 (serial) port interface. If exploited, threat actors with physical access, specialized equipment and knowledge may be able to configure or disable the pump. No electronic protected health information (ePHI), protected health information (PHI) or personally identifiable	https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/bd-bodyguard-pumps-rs-232-interface-vulnerability	H-BD-BODY-191222/870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information (PII) is stored in the pump. **CVE ID : CVE-2022-43557**		
Vendor: Broadcom					
Product: bcm5780					
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	07-Dec-2022	10	Guests can trigger NIC interface reset/abort/crash via netback It is possible for a guest to trigger a NIC interface reset/abort/crash in a Linux based network backend by sending certain kinds of packets. It appears to be an (unwritten?) assumption in the rest of the Linux network stack that packet protocol headers are all contained within the linear section of the SKB and some NICs behave badly if this is not the case. This has been reported to occur with Cisco (enic) and Broadcom NetXtrem II BCM5780 (bnx2x) though it may be an issue with other NICs/drivers as well. In case the frontend is sending requests with split headers, netback will forward those violating above mentioned assumption to the networking core,	https://xenbits.xenproject.org/xsa/advisory-423.txt	H-BRO-BCM5-191222/871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in said misbehavior. **CVE ID : CVE-2022-3643**		
Vendor: Buffalo					
Product: bhr-4grv					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-BHR--191222/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple	https://www.buffalo.jp/ne	H-BUF-BHR--191222/873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and	ws/detail/20221003-01.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: dwr-hp-g300nh					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-DWR--191222/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-DWR--191222/875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: dwr-pg					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-DWR--191222/876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-DWR--191222/877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: fs-600dhp					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-FS-6-191222/878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-FS-6-191222/879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: fs-g300n					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-FS-G-191222/880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-FS-G-191222/881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: fs-hp-g300n					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-FS-H-191222/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40966		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-FS-H-191222/883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: fs-r600dhp					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-	https://www.buffalo.jp/news/detail/20	H-BUF-FS-R-191222/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H	221003-01.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-FS-R-191222/885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: hw-450hp-zwe					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-HW-4-191222/886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-HW-4-191222/887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Use of Hard-coded Credentials	07-Dec-2022	6.5	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, and WZR-D1100H firmware Ver. 2.00 and earlier. **CVE ID : CVE-2022-34840**	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-HW-4-191222/888
Product: wcr-300					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WCR--191222/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WCR--191222/890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wem-1266					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WEM--191222/891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wem-1266wp					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WEM--191222/892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40966		
Product: wer-a54g54					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WER--191222/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WER--191222/894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wer-ag54					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WER--191222/895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WER--191222/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wer-am54g54					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WER--191222/897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WER--191222/898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wer-amg54					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WER--191222/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WER--191222/900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-300					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-300hp					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver.	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-am54g54					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-amg54					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39044		
Product: whr-ampg					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-g					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-g300n					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-g301n					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-g54s					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-g54s-ni					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver.	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-hp-ampg					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-hp-g					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39044		
Product: whr-hp-g300n					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-hp-g54					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-hp-gn					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WHR--191222/930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wlae-ag300n					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WLAE-191222/931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WLAE-191222/932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wli-h4-d600					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WLI--191222/933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WLI--191222/934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wli-tx4-ag300n					
Affected Version(s): -					
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WLI--191222/935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39044		
Product: wpl-05g300					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WPL--191222/936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WPL--191222/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wrm-d2133hp					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WRM--191222/938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wrm-d2133hs					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WRM--191222/939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: ws024bf					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WS02-191222/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40966		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WS02-191222/941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: ws024bf-nw					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-	https://www.buffalo.jp/news/detail/20	H-BUF-WS02-191222/942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H	221003-01.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WS02-191222/943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wtr-m2133hp					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WTR--191222/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wtr-m2133hs					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WTR--191222/945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40966		
Product: wxr-1750dhp					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WXR--191222/946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wxr-1750dhp2					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-	https://www.buffalo.jp/news/detail/20	H-BUF-WXR--191222/947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H	221003-01.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wxr-1900dhp					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WXR--191222/948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wxr-1900dhp2					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WXR--191222/949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wxr-1900dhp3					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WXR--191222/950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40966		
Product: wxr-5950ax12					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WXR--191222/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wxr-6000ax12b					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-	https://www.buffalo.jp/news/detail/20	H-BUF-WXR--191222/952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H	221003-01.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wxr-6000ax12s					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WXR--191222/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr-1166dhp					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr-1166dhp2					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40966		
Product: wzr-1750dhp					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr-1750dhp2					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-	https://www.buffalo.jp/news/detail/20	H-BUF-WZR--191222/957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H	221003-01.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr-300hp					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Use of Hard-coded Credentials	07-Dec-2022	6.5	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, and WZR-D1100H firmware Ver. 2.00 and earlier. **CVE ID : CVE-2022-34840**	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wzr-450hp					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Use of Hard-coded Credentials	07-Dec-2022	6.5	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, and WZR-D1100H firmware Ver. 2.00 and earlier. **CVE ID : CVE-2022-34840**		
Product: wzr-450hp-cwt					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	07-Dec-2022	6.5	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, and WZR-D1100H firmware Ver. 2.00 and earlier. **CVE ID : CVE-2022-34840**	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/966
Product: wzr-450hp-ub					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Use of Hard-coded Credentials	07-Dec-2022	6.5	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, and WZR-D1100H firmware Ver. 2.00 and earlier.	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34840		
Product: wzr-600dhp					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Use of Hard-coded Credentials	07-Dec-2022	6.5	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, and WZR-D1100H firmware Ver. 2.00 and earlier. **CVE ID : CVE-2022-34840**		
Product: wzr-600dhp2					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39044		
Use of Hard-coded Credentials	07-Dec-2022	6.5	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, and WZR-D1100H firmware Ver. 2.00 and earlier. **CVE ID : CVE-2022-34840**	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/975
Product: wzr-600dhp3					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device.	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr-900dhp					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Use of Hard-coded Credentials	07-Dec-2022	6.5	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, and WZR-D1100H firmware Ver. 2.00 and earlier. **CVE ID : CVE-2022-34840**	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/979
Product: wzr-900dhp2					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr-agl300nh					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr-ampg144nh					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr-ampg300nh					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr-d1100h					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Use of Hard-coded Credentials	07-Dec-2022	6.5	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, and WZR-D1100H firmware Ver. 2.00 and earlier. **CVE ID : CVE-2022-34840**	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/989
Product: wzr-g144n					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr-g144nh					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr-hp-ag300h					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver.	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr-hp-g300nh					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr-hp-g301nh					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39044		
Product: wzr-hp-g302h					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/1000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/1001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr-hp-g450h					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/1002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/1003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr-s1750dhp					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/1004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr-s600dhp					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/1005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr-s900dhp					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR--191222/1006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr2-g108					
Affected Version(s): -					
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR2-191222/1007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr2-g300n					
Affected Version(s): -					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR2-191222/1008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and	https://www.buffalo.jp/news/detail/20221003-01.html	H-BUF-WZR2-191222/1009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Vendor: Cisco					
Product: ata_190					
Affected Version(s): -					
Improper Input Validation	12-Dec-2022	8.8	Multiple vulnerabilities in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause Cisco Discovery Protocol memory corruption on an affected device. These vulnerabilities are due to missing length validation checks when processing Cisco Discovery Protocol messages. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read of the valid Cisco Discovery Protocol packet data, which could allow the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	H-CIS-ATA_-191222/1010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause corruption in the internal Cisco Discovery Protocol database of the affected device. **CVE ID : CVE-2022-20689**		
Improper Input Validation	12-Dec-2022	8.8	Multiple vulnerabilities in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause Cisco Discovery Protocol memory corruption on an affected device. These vulnerabilities are due to missing length validation checks when processing Cisco Discovery Protocol messages. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read of the valid Cisco Discovery Protocol packet data, which could allow the attacker to cause corruption in the internal Cisco Discovery Protocol database of the affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	H-CIS-ATA_-191222/1011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20690		
Uncontrolled Resource Consumption	12-Dec-2022	6.5	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Adaptive Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause a DoS condition of an affected device. This vulnerability is due to missing length validation of certain Cisco Discovery Protocol packet header fields. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol packets to an affected device. A successful exploit could allow the attacker to cause the device to exhaust available memory and cause the service to restart. Cisco has released firmware updates that address this vulnerability. **CVE ID : CVE-2022-20691**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	H-CIS-ATA_-191222/1012
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	5.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	H-CIS-ATA_-191222/1013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code on an affected device and cause the LLDP service to restart. These vulnerabilities are due to missing length validation of certain LLDP packet header fields. An attacker could exploit these vulnerabilities by sending a malicious LLDP packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause LLDP to restart unexpectedly, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20686**		
Improper Input Validation	12-Dec-2022	5.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause the LLDP service to restart. These vulnerabilities are due to missing length validation of certain LLDP packet header fields. An attacker could exploit these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	H-CIS-ATA_-191222/1014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities by sending a malicious LLDP packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause LLDP to restart unexpectedly, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20687**		
Improper Input Validation	12-Dec-2022	5.3	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause Cisco Discovery Protocol service to restart. This vulnerability is due to missing length validation of certain Cisco Discovery Protocol packet header fields. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause Cisco Discovery Protocol to restart unexpectedly,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	H-CIS-ATA_-191222/1015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a DoS condition. **CVE ID : CVE-2022-20688**		
Product: ata_191					
Affected Version(s): -					
Improper Input Validation	12-Dec-2022	8.8	Multiple vulnerabilities in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause Cisco Discovery Protocol memory corruption on an affected device. These vulnerabilities are due to missing length validation checks when processing Cisco Discovery Protocol messages. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read of the valid Cisco Discovery Protocol packet data, which could allow the attacker to cause corruption in the internal Cisco Discovery Protocol database of the affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	H-CIS-ATA_-191222/1016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20689		
Improper Input Validation	12-Dec-2022	8.8	Multiple vulnerabilities in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause Cisco Discovery Protocol memory corruption on an affected device. These vulnerabilities are due to missing length validation checks when processing Cisco Discovery Protocol messages. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read of the valid Cisco Discovery Protocol packet data, which could allow the attacker to cause corruption in the internal Cisco Discovery Protocol database of the affected device. **CVE ID : CVE-2022-20690**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	H-CIS-ATA_-191222/1017
Uncontrolled Resource	12-Dec-2022	6.5	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Adaptive	https://tools.cisco.com/security/center/content/Cisco	H-CIS-ATA_-191222/1018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause a DoS condition of an affected device. This vulnerability is due to missing length validation of certain Cisco Discovery Protocol packet header fields. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol packets to an affected device. A successful exploit could allow the attacker to cause the device to exhaust available memory and cause the service to restart. Cisco has released firmware updates that address this vulnerability. **CVE ID : CVE-2022-20691**	SecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	5.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause the LLDP service to restart. These vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	H-CIS-ATA_-191222/1019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing length validation of certain LLDP packet header fields. An attacker could exploit these vulnerabilities by sending a malicious LLDP packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause LLDP to restart unexpectedly, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20686**		
Improper Input Validation	12-Dec-2022	5.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause the LLDP service to restart. These vulnerabilities are due to missing length validation of certain LLDP packet header fields. An attacker could exploit these vulnerabilities by sending a malicious LLDP packet to an affected device. A successful exploit could allow the attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	H-CIS-ATA_-191222/1020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute code on the affected device and cause LLDP to restart unexpectedly, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20687**		
Improper Input Validation	12-Dec-2022	5.3	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause Cisco Discovery Protocol service to restart. This vulnerability is due to missing length validation of certain Cisco Discovery Protocol packet header fields. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause Cisco Discovery Protocol to restart unexpectedly, resulting in a DoS condition. **CVE ID : CVE-2022-20688**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	H-CIS-ATA_-191222/1021
Product: ata_192					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	12-Dec-2022	8.8	Multiple vulnerabilities in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause Cisco Discovery Protocol memory corruption on an affected device. These vulnerabilities are due to missing length validation checks when processing Cisco Discovery Protocol messages. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read of the valid Cisco Discovery Protocol packet data, which could allow the attacker to cause corruption in the internal Cisco Discovery Protocol database of the affected device. **CVE ID : CVE-2022-20689**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	H-CIS-ATA_-191222/1022
Improper Input Validation	12-Dec-2022	8.8	Multiple vulnerabilities in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone	https://tools.cisco.com/security/center/content/CiscoSecurityAdvis	H-CIS-ATA_-191222/1023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Adapter firmware could allow an unauthenticated, adjacent attacker to cause Cisco Discovery Protocol memory corruption on an affected device. These vulnerabilities are due to missing length validation checks when processing Cisco Discovery Protocol messages. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read of the valid Cisco Discovery Protocol packet data, which could allow the attacker to cause corruption in the internal Cisco Discovery Protocol database of the affected device. **CVE ID : CVE-2022-20690**	ory/cisco-sa-ata19x-multivuln-GEZYVvs	
Uncontrolled Resource Consumption	12-Dec-2022	6.5	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Adaptive Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause a DoS condition of an affected device. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	H-CIS-ATA_-191222/1024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing length validation of certain Cisco Discovery Protocol packet header fields. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol packets to an affected device. A successful exploit could allow the attacker to cause the device to exhaust available memory and cause the service to restart. Cisco has released firmware updates that address this vulnerability. **CVE ID : CVE-2022-20691**		
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	5.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause the LLDP service to restart. These vulnerabilities are due to missing length validation of certain LLDP packet header fields. An attacker could exploit these vulnerabilities by sending a malicious LLDP packet to an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	H-CIS-ATA_-191222/1025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to execute code on the affected device and cause LLDP to restart unexpectedly, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20686**		
Improper Input Validation	12-Dec-2022	5.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause the LLDP service to restart. These vulnerabilities are due to missing length validation of certain LLDP packet header fields. An attacker could exploit these vulnerabilities by sending a malicious LLDP packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause LLDP to restart unexpectedly, resulting in a denial of service (DoS) condition.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	H-CIS-ATA_-191222/1026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20687		
Improper Input Validation	12-Dec-2022	5.3	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause Cisco Discovery Protocol service to restart. This vulnerability is due to missing length validation of certain Cisco Discovery Protocol packet header fields. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause Cisco Discovery Protocol to restart unexpectedly, resulting in a DoS condition. **CVE ID : CVE-2022-20688**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	H-CIS-ATA_-191222/1027
Product: ip_phone_7811					
Affected Version(s): -					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware	https://tools.cisco.com/security/center/content/CiscoSecurityAdvis	H-CIS-IP_P-191222/1028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	ory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Product: ip_phone_7821					
Affected Version(s): -					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	H-CIS-IP_P-191222/1029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Product: ip_phone_7832					
Affected Version(s): -					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	H-CIS-IP_P-191222/1030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition on an affected device. **CVE ID : CVE-2022-20968**		
Product: ip_phone_7841					
Affected Version(s): -					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	H-CIS-IP_P-191222/1031
Product: ip_phone_7861					
Affected Version(s): -					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of	https://tools.cisco.com/security/center/	H-CIS-IP_P-191222/1032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	content/Cisco SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Product: ip_phone_8811					
Affected Version(s): -					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	H-CIS-IP_P-191222/1033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Product: ip_phone_8831					
Affected Version(s): -					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	H-CIS-IP_P-191222/1034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Product: ip_phone_8832					
Affected Version(s): -					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	H-CIS-IP_P-191222/1035
Product: ip_phone_8841					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	H-CIS-IP_P-191222/1036
Product: ip_phone_8845					
Affected Version(s): -					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	H-CIS-IP_P-191222/1037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Product: ip_phone_8851					
Affected Version(s): -					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	H-CIS-IP_P-191222/1038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Product: ip_phone_8861					
Affected Version(s): -					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	H-CIS-IP_P-191222/1039
Product: ip_phone_8865					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	H-CIS-IP_P-191222/1040
Vendor: Citrix					
Product: application_delivery_controller					
Affected Version(s): -					
N/A	13-Dec-2022	9.8	Unauthenticated remote arbitrary code execution **CVE ID : CVE-2022-27518**	https://support.citrix.com/article/CTX474995	H-CIT-APPL-191222/1041
Product: gateway					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Dec-2022	9.8	Unauthenticated remote arbitrary code execution **CVE ID : CVE-2022-27518**	https://support.citrix.com/article/CTX474995	H-CIT-GATE-191222/1042
Vendor: D-link					
Product: dhp-w310av					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	9.8	D-Link DHP-W310AV 3.10EU was discovered to contain a command injection vulnerability via the System Checks function. **CVE ID : CVE-2022-44930**	N/A	H-D-L-DHP--191222/1043
Product: dvg-g5402sp					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	9.8	D-Link DVG-G5402SP GE_1.03 was discovered to contain a command injection vulnerability via the Maintenance function. **CVE ID : CVE-2022-44928**	N/A	H-D-L-DVG--191222/1044
Improper Privilege Management	02-Dec-2022	9.8	An access control issue in D-Link DVG-G5402SP GE_1.03 allows unauthenticated attackers to escalate privileges via arbitrarily editing VoIP SIB profiles. **CVE ID : CVE-2022-44929**	N/A	H-D-L-DVG--191222/1045
Vendor: digitalalertsystems					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: dasdec_i					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-2022	5.4	A cross-site scripting (XSS) vulnerability exists in all current versions of Digital Alert Systems DASDEC software via the Host Header in undisclosed pages after login. **CVE ID : CVE-2022-40204**	https://www.digitalalertsystems.com/security-advisory	H-DIG-DASD-191222/1046
Product: dasdec_ii					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-2022	5.4	A cross-site scripting (XSS) vulnerability exists in all current versions of Digital Alert Systems DASDEC software via the Host Header in undisclosed pages after login. **CVE ID : CVE-2022-40204**	https://www.digitalalertsystems.com/security-advisory	H-DIG-DASD-191222/1047
Product: dasdec_iii					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-2022	5.4	A cross-site scripting (XSS) vulnerability exists in all current versions of Digital Alert Systems DASDEC software via the Host Header in undisclosed pages after login. **CVE ID : CVE-2022-40204**	https://www.digitalalertsystems.com/security-advisory	H-DIG-DASD-191222/1048
Product: one-net					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-2022	5.4	A cross-site scripting (XSS) vulnerability exists in all current versions of Digital Alert Systems DASDEC software via the Host Header in undisclosed pages after login. **CVE ID : CVE-2022-40204**	https://www.digitalalertsystems.com/security-advisory	H-DIG-ONE--191222/1049
Product: one-net_se					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-2022	5.4	A cross-site scripting (XSS) vulnerability exists in all current versions of Digital Alert Systems DASDEC software via the Host Header in undisclosed pages after login. **CVE ID : CVE-2022-40204**	https://www.digitalalertsystems.com/security-advisory	H-DIG-ONE--191222/1050
Vendor: dragino					
Product: lg01_lora					
Affected Version(s): -					
Files or Directories Accessible to External Parties	12-Dec-2022	7.5	The web portal of Dragino Lora LG01 18ed40 IoT v4.3.4 has the directory listing at the URL https://10.10.20.74/lib/. This address has a backup file which can be downloaded without any authentication. **CVE ID : CVE-2022-45227**	N/A	H-DRA-LG01-191222/1051
Cross-Site Request	12-Dec-2022	3.5	Dragino Lora LG01 18ed40 IoT v4.3.4 was discovered to contain a	N/A	H-DRA-LG01-191222/1052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Cross-Site Request Forgery in the logout page. **CVE ID : CVE-2022-45228**		
Vendor: Festo					
Product: bus_module_cpx-e-ep					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-BUS_-191222/1053
Product: bus_node_cpx-fb32					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-BUS_-191222/1054
Product: bus_node_cpx-fb33					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol	N/A	H-FES-BUS_-191222/1055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: bus_node_cpx-fb36					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-BUS_-191222/1056
Product: bus_node_cpx-fb37					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-BUS_-191222/1057
Product: bus_node_cpx-fb39					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a	N/A	H-FES-BUS_-191222/1058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: bus_node_cpx-fb40					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-BUS_-191222/1059
Product: bus_node_cpx-fb43					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-BUS_-191222/1060
Product: bus_node_cpx-m-fb34					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-BUS_-191222/1061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: bus_node_cpx-m-fb35					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-BUS_-191222/1062
Product: bus_node_cpx-m-fb44					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-BUS_-191222/1063
Product: bus_node_cpx-m-fb45					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-BUS_-191222/1064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: bus_node_cteu-ep					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-BUS_-191222/1065
Product: bus_node_cteu-pn					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-BUS_-191222/1066
Product: bus_node_cteu-pn-ex1c					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-BUS_-191222/1067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: camera_system_chb-c-n					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-CAME-191222/1068
Product: cecx-x-c1_modular_master_controller					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-CECX-191222/1069
Product: cecx-x-m1_modular_controller					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-CECX-191222/1070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: compact_vision_system_sboc-c					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-COMP-191222/1071
Product: compact_vision_system_sboc-m					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-COMP-191222/1072
Product: compact_vision_system_sboc-q					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-COMP-191222/1073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: compact_vision_system_sboi-c					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-COMP-191222/1074
Product: compact_vision_system_sboi-m					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-COMP-191222/1075
Product: compact_vision_system_sboi-q					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-COMP-191222/1076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: controller_cecc-d					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-CONT-191222/1077
Product: controller_cecc-d-ba					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-CONT-191222/1078
Product: controller_cecc-lk					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-CONT-191222/1079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: controller_cecc-s					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-CONT-191222/1080
Product: controller_cecc-x-m1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-CONT-191222/1081
Product: controller_cecc-x-m1-mv					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-CONT-191222/1082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: controller_cecc-x-m1-mv-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-CONT-191222/1083
Product: controller_cecc-x-m1-y-yjkp					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-CONT-191222/1084
Product: controller_cecc-x-m1-ys-l1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-CONT-191222/1085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: controller_cecc-x-m1-ys-l2					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-CONT-191222/1086
Product: controller_cmxh-st2-c5-7-diop					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-CONT-191222/1087
Product: controller_sbrd-q					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-CONT-191222/1088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: control_block_cpx-cec					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-CONT-191222/1089
Product: control_block_cpx-cec-c1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-CONT-191222/1090
Product: control_block_cpx-cec-c1-v3					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-CONT-191222/1091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: control_block_cpx-cec-m1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-CONT-191222/1092
Product: control_block_cpx-cec-m1-v3					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-CONT-191222/1093
Product: control_block_cpx-cec-s1-v3					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-CONT-191222/1094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: control_block_cpx-cmxx					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-CONT-191222/1095
Product: control_block_cpx-fec-1-ie					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-CONT-191222/1096
Product: ethernet\/ip_interface_cpx-ap-i-ep-m12					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-ETHE-191222/1097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: ethernet\/ip_interface_cpx-ap-i-pn-m12					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-ETHE-191222/1098
Product: gateway_cpx-iot					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-GATE-191222/1099
Product: integrated_drive_emca-ec-67					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-INTE-191222/1100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: integrated_drive_emca-ec-67-m-1te-ep					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-INTE-191222/1101
Product: motor_controller_cmmo-st-c5-1-dion					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-MOTO-191222/1102
Product: motor_controller_cmmo-st-c5-1-diop					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-MOTO-191222/1103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: motor_controller_cmmo-st-c5-1-lkp					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-MOTO-191222/1104
Product: motor_controller_cmmp-as-c10-11a-p3-m0					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-MOTO-191222/1105
Product: motor_controller_cmmp-as-c10-11a-p3-m3					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-MOTO-191222/1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: motor_controller_cmmp-as-c15-11a-p3-m3					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-MOTO-191222/1107
Product: motor_controller_cmmp-as-c2-3a-m0					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-MOTO-191222/1108
Product: motor_controller_cmmp-as-c2-3a-m3					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-MOTO-191222/1109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: motor_controller_cmmp-as-c5-11a-p3-m0					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-MOTO-191222/1110
Product: motor_controller_cmmp-as-c5-11a-p3-m3					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-MOTO-191222/1111
Product: motor_controller_cmmp-as-c5-3a-m0					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-MOTO-191222/1112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: motor_controller_cmmp-as-c5-3a-m3					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-MOTO-191222/1113
Product: operator_unit_cdpx-x-a-s-10					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-OPER-191222/1114
Product: operator_unit_cdpx-x-a-w-13					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-OPER-191222/1115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: operator_unit_cdpx-x-a-w-4					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-OPER-191222/1116
Product: operator_unit_cdpx-x-a-w-7					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-OPER-191222/1117
Product: planar_surface_gantry_excm-30					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-PLAN-191222/1118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: planar_surface_gantry_excm-40					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-PLAN-191222/1119
Product: servo_cmmt-as-c12-11a-p3-ec-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1120
Product: servo_cmmt-as-c12-11a-p3-ep-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-SERV-191222/1121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: servo_cmmt-as-c12-11a-p3-mp-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1122
Product: servo_cmmt-as-c12-11a-p3-pn-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1123
Product: servo_cmmt-as-c2-11a-p3-ec-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-SERV-191222/1124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: servo_cmmt-as-c2-11a-p3-ep-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1125
Product: servo_cmmt-as-c2-11a-p3-mp-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1126
Product: servo_cmmt-as-c2-11a-p3-pn-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-SERV-191222/1127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: servo_cmmt-as-c2-3a-ec-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1128
Product: servo_cmmt-as-c2-3a-ep-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1129
Product: servo_cmmt-as-c2-3a-mp-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-SERV-191222/1130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: servo_cmmt-as-c2-3a-pn-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1131
Product: servo_cmmt-as-c3-11a-p3-ec-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1132
Product: servo_cmmt-as-c3-11a-p3-ep-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-SERV-191222/1133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: servo_cmmt-as-c3-11a-p3-mp-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1134
Product: servo_cmmt-as-c3-11a-p3-pn-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1135
Product: servo_cmmt-as-c4-3a-ec-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-SERV-191222/1136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: servo_cmmt-as-c4-3a-ep-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1137
Product: servo_cmmt-as-c4-3a-mp-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1138
Product: servo_cmmt-as-c4-3a-pn-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-SERV-191222/1139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: servo_cmmt-as-c5-11a-p3-ec-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1140
Product: servo_cmmt-as-c5-11a-p3-ep-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1141
Product: servo_cmmt-as-c5-11a-p3-mp-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-SERV-191222/1142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: servo_cmmt-as-c5-11a-p3-pn-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1143
Product: servo_cmmt-as-c7-11a-p3-ec-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1144
Product: servo_cmmt-as-c7-11a-p3-ep-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-SERV-191222/1145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: servo_cmmt-as-c7-11a-p3-mp-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1146
Product: servo_cmmt-as-c7-11a-p3-pn-s1					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1147
Product: servo_drive_cmmt-st-c8-1c-ep-s0					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-SERV-191222/1148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Product: servo_drive_cmmt-st-c8-1c-pn-s0					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-SERV-191222/1149
Product: vtem-s1-27					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	H-FES-VTEM-191222/1150
Product: vtem-s1-c					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of	N/A	H-FES-VTEM-191222/1151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**		
Vendor: flir					
Product: flir_ax8					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Dec-2022	9.8	A vulnerability classified as critical has been found in Teledyne FLIR AX8 up to 1.46.16. Affected is an unknown function of the file palette.php of the component Web Service Handler. The manipulation of the argument palette leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-215118 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4364**	N/A	H-FLI-FLIR-191222/1152
Vendor: force1rc					
Product: discovery_wifi_u818a_hd\+_fpv					
Affected Version(s): -					
Out-of-bounds Write	06-Dec-2022	9.8	Buffer overflow in firmware lewei_cam binary version 2.0.10 in Force 1 Discovery Wifi U818A HD+ FPV Drone allows attacker to gain remote code execution as root user via a specially crafted UDP packet. Please update the	N/A	H-FOR-DISC-191222/1153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Reference section to these links > http://thiscomputer.com/ > https://www.bostoncyber.org/ > https://medium.com/@meekworth/exploiting-the-lw9621-drone-camera-module-773f00081368 **CVE ID : CVE-2022-40918**		
Vendor: fsi					
Product: fs020w					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	05-Dec-2022	7.3	Cross-site request forgery (CSRF) vulnerability in +F FS040U software versions v2.3.4 and earlier, +F FS020W software versions v4.0.0 and earlier, +F FS030W software versions v3.3.5 and earlier, and +F FS040W software versions v1.4.1 and earlier allows an adjacent attacker to hijack the authentication of an administrator and user's unintended operations such as to reboot the product and/or reset the configuration to the initial set-up may be performed. **CVE ID : CVE-2022-43470**	https://www.fsi.co.jp/mobile/plusF/news/22102803.html, https://www.fsi.co.jp/mobile/plusF/news/22102802.html, https://www.fsi.co.jp/mobile/plusF/news/22102804.html, https://www.fsi.co.jp/mobile/plusF/news/22102801.html	H-FSI-FS02-191222/1154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: fs030w					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	05-Dec-2022	7.3	Cross-site request forgery (CSRF) vulnerability in +F FS040U software versions v2.3.4 and earlier, +F FS020W software versions v4.0.0 and earlier, +F FS030W software versions v3.3.5 and earlier, and +F FS040W software versions v1.4.1 and earlier allows an adjacent attacker to hijack the authentication of an administrator and user's unintended operations such as to reboot the product and/or reset the configuration to the initial set-up may be performed. **CVE ID : CVE-2022-43470**	https://www.fsi.co.jp/mobile/plusF/news/22102803.html, https://www.fsi.co.jp/mobile/plusF/news/22102802.html, https://www.fsi.co.jp/mobile/plusF/news/22102804.html, https://www.fsi.co.jp/mobile/plusF/news/22102801.html	H-FSI-FS03-191222/1155
Product: fs040u					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	05-Dec-2022	7.3	Cross-site request forgery (CSRF) vulnerability in +F FS040U software versions v2.3.4 and earlier, +F FS020W software versions v4.0.0 and earlier, +F FS030W software versions v3.3.5 and earlier, and +F FS040W software versions v1.4.1 and earlier allows an	https://www.fsi.co.jp/mobile/plusF/news/22102803.html, https://www.fsi.co.jp/mobile/plusF/news/22102802.html, https://www.fsi.co.jp/mobile/plusF/news	H-FSI-FS04-191222/1156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to hijack the authentication of an administrator and user's unintended operations such as to reboot the product and/or reset the configuration to the initial set-up may be performed. **CVE ID : CVE-2022-43470**	/22102804.html, https://www.fsi.co.jp/mobile/plusF/news/22102801.html	
Insufficiently Protected Credentials	05-Dec-2022	4.6	Plaintext storage of a password vulnerability exists in +F FS040U software versions v2.3.4 and earlier, which may allow an attacker to obtain the login password of +F FS040U and log in to the management console. **CVE ID : CVE-2022-43442**	https://www.fsi.co.jp/mobile/plusF/news/22102803.html, https://www.fsi.co.jp/mobile/plusF/news/22102802.html, https://www.fsi.co.jp/mobile/plusF/news/22102804.html, https://www.fsi.co.jp/mobile/plusF/news/22102801.html	H-FSI-FS04-191222/1157
Product: fs040w					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	05-Dec-2022	7.3	Cross-site request forgery (CSRF) vulnerability in +F FS040U software versions v2.3.4 and earlier, +F FS020W software versions v4.0.0 and earlier, +F FS030W	https://www.fsi.co.jp/mobile/plusF/news/22102803.html, https://www.fsi.co.jp/mobile/plusF/news	H-FSI-FS04-191222/1158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software versions v3.3.5 and earlier, and +F FS040W software versions v1.4.1 and earlier allows an adjacent attacker to hijack the authentication of an administrator and user's unintended operations such as to reboot the product and/or reset the configuration to the initial set-up may be performed. **CVE ID : CVE-2022-43470**	/22102802.html, https://www.fsi.co.jp/mobile/plusF/news/22102804.html, https://www.fsi.co.jp/mobile/plusF/news/22102801.html	
Vendor: hornerautomation					
Product: rcc972					
Affected Version(s): -					
Use of Hard-coded Cryptographic Key	02-Dec-2022	9.8	Horner Automation's RCC 972 with firmware version 15.40 has a static encryption key on the device. This could allow an attacker to perform unauthorized changes to the device, remotely execute arbitrary code, or cause a denial-of-service condition. **CVE ID : CVE-2022-2641**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-335-02	H-HOR-RCC9-191222/1159
Inadequate Encryption Strength	02-Dec-2022	7.5	The Config-files of Horner Automation's RCC 972 with firmware version 15.40 are encrypted with weak XOR encryption vulnerable to reverse engineering. This could allow an attacker to	https://www.cisa.gov/uscert/ics/advisories/icsa-22-335-02	H-HOR-RCC9-191222/1160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			obtain credentials to run services such as File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP). **CVE ID : CVE-2022-2640**		
Excessive Reliance on Global Variables	02-Dec-2022	7.5	Horner Automation's RCC 972 firmware version 15.40 contains global variables. This could allow an attacker to read out sensitive values and variable keys from the device. **CVE ID : CVE-2022-2642**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-335-02	H-HOR-RCC9-191222/1161
Vendor: HP					
Product: m2u75a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U7-191222/1162
Product: m2u76a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U7-191222/1163
Product: m2u77a					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U7-191222/1164
Product: m2u81a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U8-191222/1165
Product: m2u81b					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U8-191222/1166
Product: m2u82a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U8-191222/1167
Product: m2u82b					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet	https://support.hp.com/us-	H-HP-M2U8-191222/1168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	en/document/ish_7095452-7095489-16/hpsbpi03813	
Product: m2u84a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U8-191222/1169
Product: m2u84b					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U8-191222/1170
Product: m2u85a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U8-191222/1171
Product: m2u85b					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be	https://support.hp.com/us-en/document/ish_7095452	H-HP-M2U8-191222/1172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	-7095489-16/hpsbpi03813	
Product: m2u86a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U8-191222/1173
Product: m2u86b					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U8-191222/1174
Product: m2u86c					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U8-191222/1175
Product: m2u87a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack.	https://support.hp.com/us-en/document/ish_7095452-7095489-	H-HP-M2U8-191222/1176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43780	16/hpsbpi03813	
Product: m2u87b					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U8-191222/1177
Product: m2u88b					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U8-191222/1178
Product: m2u89b					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U8-191222/1179
Product: m2u91a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U9-191222/1180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: m2u91b					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U9-191222/1181
Product: m2u92a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U9-191222/1182
Product: m2u92b					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U9-191222/1183
Product: m2u94a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U9-191222/1184
Product: m2u94b					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-M2U9-191222/1185
Product: pagewide_352dw_j6u57a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	H-HP-PAGE-191222/1186
Product: pagewide_377dw_j9v80a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	H-HP-PAGE-191222/1187
Product: pagewide_managed_p55250dw_j6u51b					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	H-HP-PAGE-191222/1188
Product: pagewide_managed_p55250dw_j6u55a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be	https://support.hp.com/us-en/document	H-HP-PAGE-191222/1189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	/ish_6720386-6720411-16/hpsbpi03807	
Product: pagewide_managed_p55250dw_j6u55b					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	H-HP-PAGE-191222/1190
Product: pagewide_managed_p57750dw_j9v82a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	H-HP-PAGE-191222/1191
Product: pagewide_pro_452dn_d3q15a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	H-HP-PAGE-191222/1192
Product: pagewide_pro_452dw_d3q16a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-	H-HP-PAGE-191222/1193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				16/hpsbpi03807	
Product: pagewide_pro_477dn_d3q19a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	H-HP-PAGE-191222/1194
Product: pagewide_pro_477dw_d3q20a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	H-HP-PAGE-191222/1195
Product: pagewide_pro_552dw_d3q17a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	H-HP-PAGE-191222/1196
Product: pagewide_pro_577dw_d3q21a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	H-HP-PAGE-191222/1197
Product: pagewide_pro_577z_k9z76a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	H-HP-PAGE-191222/1198
Product: z4a54a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-Z4A5-191222/1199
Product: z4a59a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-Z4A5-191222/1200
Product: z4a60a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-Z4A6-191222/1201
Product: z4a61a					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-Z4A6-191222/1202
Product: z4a61b					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-Z4A6-191222/1203
Product: z4a69a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-Z4A6-191222/1204
Product: z4a70a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-Z4A7-191222/1205
Product: z4a71a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet	https://support.hp.com/us-	H-HP-Z4A7-191222/1206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	en/document/ish_7095452-7095489-16/hpsbpi03813	
Product: z4a73a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-Z4A7-191222/1207
Product: z4a74a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-Z4A7-191222/1208
Product: z4b12a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-Z4B1-191222/1209
Product: z4b13a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be	https://support.hp.com/us-en/document/ish_7095452	H-HP-Z4B1-191222/1210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	-7095489-16/hpsbpi03813	
Product: z4b14a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-Z4B1-191222/1211
Product: z4b18a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-Z4B1-191222/1212
Product: z4b27a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-Z4B2-191222/1213
Product: z4b28a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack.	https://support.hp.com/us-en/document/ish_7095452-7095489-	H-HP-Z4B2-191222/1214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43780	16/hpsbpi03813	
Product: z4b29a					
Affected Version(s): -					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	H-HP-Z4B2-191222/1215
Vendor: hpe					
Product: hf20					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	H-HPE-HF20-191222/1216
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	H-HPE-HF20-191222/1217
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na	H-HPE-HF20-191222/1218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	- hpesbst04361en_us	
Product: hf20c					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	H-HPE-HF20-191222/1219
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	H-HPE-HF20-191222/1220
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	H-HPE-HF20-191222/1221
Product: hf20h					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	H-HPE-HF20-191222/1222
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	H-HPE-HF20-191222/1223
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	H-HPE-HF20-191222/1224
Product: hf40					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-HF40-191222/1225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37928	hpesbst04359en_us	
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	H-HPE-HF40-191222/1226
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	H-HPE-HF40-191222/1227
Product: hf40c					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	H-HPE-HF40-191222/1228
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na	H-HPE-HF40-191222/1229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	-hpesbst04360en_us	
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	H-HPE-HF40-191222/1230
Product: hf60					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	H-HPE-HF60-191222/1231
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	H-HPE-HF60-191222/1232
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and	https://support.hpe.com/hpsc/doc/public/display?docL	H-HPE-HF60-191222/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	ocale=en_US&docId=emr_na-hpesbst04361en_us	
Product: hf60c					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	H-HPE-HF60-191222/1234
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	H-HPE-HF60-191222/1235
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	H-HPE-HF60-191222/1236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sf100					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	H-HPE-SF10-191222/1237
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	H-HPE-SF10-191222/1238
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	H-HPE-SF10-191222/1239
Product: sf300					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na	H-HPE-SF30-191222/1240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	- hpesbst04359en_us	
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	H-HPE-SF30-191222/1241
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	H-HPE-SF30-191222/1242
Vendor: IBM					
Product: power_system_ac922_\(8335-gtg\)					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	12-Dec-2022	4.9	IBM OpenBMC OP910 and OP940 could allow a privileged user to cause a denial of service by uploading or deleting too many CA certificates in a short period of time. IBM X-Force ID: 2226337. **CVE ID : CVE-2022-22488**	https://exchange.xforce.ibmcloud.com/vulnerabilities/226337, https://www.ibm.com/support/pages/node/6840155	H-IBM-POWE-191222/1243
Product: power_system_ac922_\(8335-gth\)					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	12-Dec-2022	4.9	IBM OpenBMC OP910 and OP940 could allow a privileged user to cause a denial of service by uploading or deleting too many CA certificates in a short period of time. IBM X-Force ID: 2226337. **CVE ID : CVE-2022-22488**	https://exchange.xforce.ibmcloud.com/vulnerabilities/226337, https://www.ibm.com/support/pages/node/6840155	H-IBM-POWE-191222/1244
Product: power_system_ac922_\(8335-gtx\)					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	12-Dec-2022	4.9	IBM OpenBMC OP910 and OP940 could allow a privileged user to cause a denial of service by uploading or deleting too many CA certificates in a short period of time. IBM X-Force ID: 2226337. **CVE ID : CVE-2022-22488**	https://exchange.xforce.ibmcloud.com/vulnerabilities/226337, https://www.ibm.com/support/pages/node/6840155	H-IBM-POWE-191222/1245
Vendor: ifm					
Product: moneo_qha200					
Affected Version(s): -					
Weak Password Recovery Mechanism for Forgotten Password	12-Dec-2022	7.5	In IFM Moneo Appliance with version up to 1.9.3 an unauthenticated remote attacker can reset the administrator password by only supplying the serial number. **CVE ID : CVE-2022-3485**	N/A	H-IFM-MONE-191222/1246
Product: moneo_qha210					
Affected Version(s): -					
Weak Password	12-Dec-2022	7.5	In IFM Moneo Appliance with version up to 1.9.3	N/A	H-IFM-MONE-191222/1247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Recovery Mechanism for Forgotten Password			an unauthenticated remote attacker can reset the administrator password by only supplying the serial number. **CVE ID : CVE-2022-3485**		
Vendor: Kyocera					
Product: ecosys_m2535dn					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-ECOS-191222/1248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100 DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-ECOS-191222/1249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			C5250DN, LS-4300DN/4200DN/2100 DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100 DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN.	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-ECOS-191222/1250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41830		
Product: ecosys_m6526cdn					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN.	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-ECOS-191222/1251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41798		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-ECOS-191222/1252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-ECOS-191222/1253
Product: ecosys_m6526cidn					
Affected Version(s): -					
Authentication	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in	https://www.kyoceradocumentsolutions	H-KYO-ECOS-191222/1254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bypass by Spoofing			Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may	https://www.kyoceradocumentsolutions.co.jp/support/information/	H-KYO-ECOS-191222/1255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Improper Neutralization of Input During Web Page Generation	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp	H-KYO-ECOS-191222/1256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	/en/jp/JVN46345126/index.html	
Product: ecosys_p2135dn					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information.	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46	H-KYO-ECOS-191222/1257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	345126/index.html	
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-ECOS-191222/1258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-ECOS-191222/1259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: ecosys_p4040dn					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-ECOS-191222/1260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-ECOS-191222/1261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-ECOS-191222/1262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: ecosys_p6026cdn					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-ECOS-191222/1263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-ECOS-191222/1264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-ECOS-191222/1265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4300DN/4200DN/2100 DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: fs-1370dn					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-FS-1-191222/1266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4300DN/4200DN/2100 DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100 DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-FS-1-191222/1267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-FS-1-191222/1268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: fs-c2026mfp					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-FS-C-191222/1269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-FS-C-191222/1270
Improper Neutralization of	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document	https://www.kyoceradocumentsolutions	H-KYO-FS-C-191222/1271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Product: fs-c2126mfp					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may	https://www.kyoceradocumentsolutions.co.jp/support/information/info_2022110	H-KYO-FS-C-191222/1272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	1.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp	H-KYO-FS-C-191222/1273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	/en/jp/JVN46345126/index.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-FS-C-191222/1274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: fs-c2126mfp\+					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-FS-C-191222/1275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-FS-C-191222/1276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-FS-C-191222/1277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: fs-c5250dn					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-FS-C-191222/1278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-FS-C-191222/1279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-FS-C-191222/1280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: ls-1035mfp					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-1-191222/1281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-1-191222/1282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-1-191222/1283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: ls-1135mfp					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-1-191222/1284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN.	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-1-191222/1285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41807		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-1-191222/1286
Product: ls-2100dn					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-2-191222/1287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-2-191222/1288
Improper Neutralization of	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document	https://www.kyoceradocumentsolutions	H-KYO-LS-2-191222/1289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Product: ls-3140mfp					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may	https://www.kyoceradocumentsolutions.co.jp/support/information/info_2022110	H-KYO-LS-3-191222/1290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	1.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp	H-KYO-LS-3-191222/1291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	/en/jp/JVN46345126/index.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-3-191222/1292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: ls-3140mfp\+					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-3-191222/1293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-3-191222/1294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-3-191222/1295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: ls-3640mfp					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-3-191222/1296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-3-191222/1297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-3-191222/1298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: ls-4200dn					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-4-191222/1299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-4-191222/1300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-4-191222/1301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: ls-4300dn					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-4-191222/1302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN.	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-4-191222/1303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41807		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-4-191222/1304
Product: ls-c8600dn					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-C-191222/1305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-C-191222/1306
Improper Neutralization of	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document	https://www.kyoceradocumentsolutions	H-KYO-LS-C-191222/1307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Product: ls-c8650dn					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may	https://www.kyoceradocumentsolutions.co.jp/support/information/info_2022110	H-KYO-LS-C-191222/1308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	1.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp	H-KYO-LS-C-191222/1309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	/en/jp/JVN46345126/index.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-LS-C-191222/1310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_205c					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_206ci					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_255					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_255c					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN.	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41807		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1322
Product: taskalfa_256ci					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1324
Improper Neutralization of	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document	https://www.kyoceradocumentsolutions	H-KYO-TASK-191222/1325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Product: taskalfa_256i					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may	https://www.kyoceradocumentsolutions.co.jp/support/information/info_2022110	H-KYO-TASK-191222/1326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	1.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp	H-KYO-TASK-191222/1327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	/en/jp/JVN46345126/index.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_305					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_3050ci					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_306i					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_3500i					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN.	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41807		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1340
Product: taskalfa_3550ci					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1342
Improper Neutralization of	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document	https://www.kyoceradocumentsolutions	H-KYO-TASK-191222/1343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Product: taskalfa_4500i					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may	https://www.kyoceradocumentsolutions.co.jp/support/information/info_2022110	H-KYO-TASK-191222/1344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	1.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp	H-KYO-TASK-191222/1345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	/en/jp/JVN46345126/index.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_4550ci					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_5500i					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_5550ci					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_6500i					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN.	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41807		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1358
Product: taskalfa_6550ci					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1360
Improper Neutralization of	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document	https://www.kyoceradocumentsolutions	H-KYO-TASK-191222/1361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Product: taskalfa_7550ci					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may	https://www.kyoceradocumentsolutions.co.jp/support/information/info_2022110	H-KYO-TASK-191222/1362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	1.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp	H-KYO-TASK-191222/1363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	/en/jp/JVN46345126/index.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_8000i					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	H-KYO-TASK-191222/1367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Vendor: mediatek					
Product: m6833					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In isp, 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. Patch ID: ALPS07310780; Issue ID: ALPS07310780. **CVE ID : CVE-2022-32628**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-M683-191222/1368
Out-of-bounds Write	05-Dec-2022	6.7	In isp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-	H-MED-M683-191222/1369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310774; Issue ID: ALPS07310774. **CVE ID : CVE-2022-32629**	bulletin/December-2022	
Product: mt6580					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT65-191222/1370
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT65-191222/1371
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, there is a possible out of bounds write due to improper	https://corp.mediatek.com/product-	H-MED-MT65-191222/1372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	security-bulletin/December-2022	
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT65-191222/1373
Product: mt6731					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt6735					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1375
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1376
Product: mt6737					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**		
Product: mt6739					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1378
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1379
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**		
Product: mt6753					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1381
Product: mt6757					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt6757c					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1383
Product: mt6757cd					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1384
Product: mt6757ch					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**		
Product: mt6761					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1386
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1387
Out-of-bounds Write	05-Dec-2022	6.7	In display, there is a possible out of bounds write due to an incorrect bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-191222/1388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**	bulletin/December-2022	
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1389
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1390
Improper Input Validation	05-Dec-2022	6.7	In ccci, there is a possible out of bounds write due to improper input validation. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-191222/1391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	bulletin/December-2022	
Product: mt6762					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1392
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1394
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1395
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1397
Product: mt6763					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1398
Product: mt6765					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1400
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1401
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**		
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1403
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1404
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**		
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1406
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1407
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**		
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1409
Product: mt6768					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1410
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1412
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1413
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**		
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1415
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1416
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**		
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1418
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1419
Improper Input Validation	05-Dec-2022	6.7	In ccci, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**		
Product: mt6769					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1421
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1422
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, there is a possible out of bounds write due to an incorrect	https://corp.mediatek.com/product-	H-MED-MT67-191222/1423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	security-bulletin/December-2022	
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1424
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1425
Improper Privilege	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic	https://corp.mediatek.com/product-	H-MED-MT67-191222/1426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	security-bulletin/December-2022	
Product: mt6771					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1427
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1429
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1430
Product: mt6779					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32594		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1432
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1433
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32598		
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1435
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1436
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326239; Issue ID: ALPS07326239.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32626		
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1438
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1439
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32633		
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1441
Product: mt6781					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1442
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1444
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1445
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**		
Out-of-bounds Write	05-Dec-2022	6.7	In mpu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07541753; Issue ID: ALPS07541753. **CVE ID : CVE-2022-32620**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1447
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1448
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**		
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1450
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1451
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**		
Product: mt6785					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1453
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1454
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1456
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1457
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**		
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1459
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1460
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**		
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1462
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1463
Product: mt6789					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, there is a possible out of bounds write due to an incorrect bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-191222/1464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	bulletin/December-2022	
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1465
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1466
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, there is a possible out of bounds write due to an incorrect bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-191222/1467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	bulletin/December-2022	
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1468
Out-of-bounds Write	05-Dec-2022	6.7	In mpu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07541753; Issue ID: ALPS07541753. **CVE ID : CVE-2022-32620**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1469
Out-of-bounds Write	05-Dec-2022	6.7	In gz, there is a possible memory corruption due to a missing bounds check. This could lead to	https://corp.mediatek.com/product-security-	H-MED-MT67-191222/1470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363786; Issue ID: ALPS07363786. **CVE ID : CVE-2022-32622**	bulletin/December-2022	
Out-of-bounds Write	05-Dec-2022	6.7	In throttling, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405923; Issue ID: ALPS07405923. **CVE ID : CVE-2022-32624**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1471
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1472
Out-of-bounds Write	05-Dec-2022	6.7	In display, there is a possible out of bounds write due to an incorrect bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-191222/1473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**	bulletin/December-2022	
Out-of-bounds Write	05-Dec-2022	6.7	In throttling, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405966; Issue ID: ALPS07405966. **CVE ID : CVE-2022-32630**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1474
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT67-191222/1475
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to	https://corp.mediatek.com/product-security-	H-MED-MT67-191222/1476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	bulletin/December-2022	
Product: mt6833					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1477
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1479
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1480
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Dec-2022	6.7	In mpu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07541753; Issue ID: ALPS07541753. **CVE ID : CVE-2022-32620**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1482
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1483
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1485
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1486
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1488
Product: mt6853					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1489
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32596		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1491
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1492
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32619		
Out-of-bounds Write	05-Dec-2022	6.7	In mpu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07541753; Issue ID: ALPS07541753. **CVE ID : CVE-2022-32620**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1494
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1495
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326239; Issue ID: ALPS07326239.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32626		
Out-of-bounds Write	05-Dec-2022	6.7	In isp, 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. Patch ID: ALPS07310780; Issue ID: ALPS07310780. **CVE ID : CVE-2022-32628**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1497
Out-of-bounds Write	05-Dec-2022	6.7	In isp, 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. Patch ID: ALPS07310774; Issue ID: ALPS07310774. **CVE ID : CVE-2022-32629**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1498
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32631		
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1500
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1501
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32634		
Product: mt6853t					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1503
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1504
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1506
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1507
Product: mt6855					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1509
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1510
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**		
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1512
Out-of-bounds Write	05-Dec-2022	6.7	In gz, there is a possible memory corruption 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. Patch ID: ALPS07363786; Issue ID: ALPS07363786. **CVE ID : CVE-2022-32622**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1513
Out-of-bounds Write	05-Dec-2022	6.7	In throttling, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405923; Issue ID: ALPS07405923. **CVE ID : CVE-2022-32624**		
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1515
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1516
Out-of-bounds Write	05-Dec-2022	6.7	In isp, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07310780; Issue ID: ALPS07310780. **CVE ID : CVE-2022-32628**		
Out-of-bounds Write	05-Dec-2022	6.7	In isp, 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. Patch ID: ALPS07310774; Issue ID: ALPS07310774. **CVE ID : CVE-2022-32629**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1518
Out-of-bounds Write	05-Dec-2022	6.7	In throttling, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405966; Issue ID: ALPS07405966. **CVE ID : CVE-2022-32630**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1519
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**		
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1521
Product: mt6873					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1522
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, there is a possible out of bounds write due to an incorrect bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-191222/1523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	bulletin/December-2022	
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1524
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1525
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, there is a possible out of bounds write due to an incorrect bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-191222/1526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	bulletin/December-2022	
Out-of-bounds Write	05-Dec-2022	6.7	In mpu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07541753; Issue ID: ALPS07541753. **CVE ID : CVE-2022-32620**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1527
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1528
Out-of-bounds Write	05-Dec-2022	6.7	In display, there is a possible out of bounds write due to an incorrect bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-191222/1529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**	bulletin/December-2022	
Out-of-bounds Write	05-Dec-2022	6.7	In isp, 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. Patch ID: ALPS07310780; Issue ID: ALPS07310780. **CVE ID : CVE-2022-32628**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1530
Out-of-bounds Write	05-Dec-2022	6.7	In isp, 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. Patch ID: ALPS07310774; Issue ID: ALPS07310774. **CVE ID : CVE-2022-32629**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1531
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, there is a possible out of bounds write due to improper input validation. This	https://corp.mediatek.com/product-security-	H-MED-MT68-191222/1532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	bulletin/December-2022	
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1533
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1534
Improper Input Validation	05-Dec-2022	6.7	In ccci, there is a possible out of bounds write due to improper input validation. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-191222/1535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	bulletin/December-2022	
Product: mt6875					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1536
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1538
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1539
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1541
Product: mt6877					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1542
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32596		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1544
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1545
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32619		
Out-of-bounds Write	05-Dec-2022	6.7	In mpu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07541753; Issue ID: ALPS07541753. **CVE ID : CVE-2022-32620**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1547
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1548
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326239; Issue ID: ALPS07326239.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32626		
Out-of-bounds Write	05-Dec-2022	6.7	In isp, 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. Patch ID: ALPS07310780; Issue ID: ALPS07310780. **CVE ID : CVE-2022-32628**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1550
Out-of-bounds Write	05-Dec-2022	6.7	In isp, 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. Patch ID: ALPS07310774; Issue ID: ALPS07310774. **CVE ID : CVE-2022-32629**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1551
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32631		
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1553
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1554
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32634		
Product: mt6879					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1556
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1557
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1559
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1560
Out-of-bounds Write	05-Dec-2022	6.7	In gz, there is a possible memory corruption 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07363786; Issue ID: ALPS07363786. **CVE ID : CVE-2022-32622**		
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1562
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1563
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**		
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1565
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1566
Product: mt6883					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1568
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1569
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**		
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1571
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1572
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**		
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1574
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1575
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**		
Product: mt6885					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1577
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1578
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, there is a possible out of bounds write due to an incorrect bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-191222/1579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	bulletin/December-2022	
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1580
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1581
Out-of-bounds Write	05-Dec-2022	6.7	In display, there is a possible out of bounds write due to an incorrect bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-191222/1582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	bulletin/December-2022	
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1583
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1584
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to	https://corp.mediatek.com/product-security-	H-MED-MT68-191222/1585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	bulletin/December-2022	
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1586
Product: mt6889					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1588
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1589
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1591
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1592
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1594
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1595
Product: mt6891					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32594		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1597
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1598
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32598		
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1600
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1601
Product: mt6893					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1603
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1604
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**		
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1606
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1607
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**		
Out-of-bounds Write	05-Dec-2022	6.7	In isp, 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. Patch ID: ALPS07310780; Issue ID: ALPS07310780. **CVE ID : CVE-2022-32628**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1609
Out-of-bounds Write	05-Dec-2022	6.7	In isp, 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. Patch ID: ALPS07310774; Issue ID: ALPS07310774. **CVE ID : CVE-2022-32629**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1610
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**		
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1612
Product: mt6895					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1613
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1615
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1616
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**		
Out-of-bounds Write	05-Dec-2022	6.7	In gz, there is a possible memory corruption 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. Patch ID: ALPS07363786; Issue ID: ALPS07363786. **CVE ID : CVE-2022-32622**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1618
Out-of-bounds Write	05-Dec-2022	6.7	In throttling, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405923; Issue ID: ALPS07405923. **CVE ID : CVE-2022-32624**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1619
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**		
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1621
Out-of-bounds Write	05-Dec-2022	6.7	In throttling, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405966; Issue ID: ALPS07405966. **CVE ID : CVE-2022-32630**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1622
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**		
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1624
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1625
Concurrent Execution using Shared Resource with Improper	05-Dec-2022	6.4	In isp, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT68-191222/1626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			interaction is not needed for exploitation. Patch ID: ALPS07310829; Issue ID: ALPS07310829. **CVE ID : CVE-2022-32621**		
Product: mt6983					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT69-191222/1627
Out-of-bounds Write	05-Dec-2022	6.7	In gz, there is a possible memory corruption 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. Patch ID: ALPS07363786; Issue ID: ALPS07363786. **CVE ID : CVE-2022-32622**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT69-191222/1628
Out-of-bounds Write	05-Dec-2022	6.7	In throttling, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT69-191222/1629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405923; Issue ID: ALPS07405923. **CVE ID : CVE-2022-32624**	bulletin/December-2022	
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT69-191222/1630
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT69-191222/1631
Out-of-bounds Write	05-Dec-2022	6.7	In throttling, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT69-191222/1632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405966; Issue ID: ALPS07405966. **CVE ID : CVE-2022-32630**	bulletin/December-2022	
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT69-191222/1633
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT69-191222/1634
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of	https://corp.mediatek.com/product-security-	H-MED-MT69-191222/1635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	bulletin/December-2022	
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT69-191222/1636
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	05-Dec-2022	6.4	In isp, there is a possible out of bounds write 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. Patch ID: ALPS07310829; Issue ID: ALPS07310829. **CVE ID : CVE-2022-32621**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT69-191222/1637
Product: mt7663					
Affected Version(s): -					
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, there is a possible out of bounds write due to improper	https://corp.mediatek.com/product-	H-MED-MT76-191222/1638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	security-bulletin/December-2022	
Product: mt7668					
Affected Version(s): -					
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT76-191222/1639
Product: mt7902					
Affected Version(s): -					
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT79-191222/1640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32632		
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT79-191222/1641
Product: mt7921					
Affected Version(s): -					
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT79-191222/1642
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT79-191222/1643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**		
Product: mt7933					
Affected Version(s): -					
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT79-191222/1644
Product: mt8167s					
Affected Version(s): -					
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT81-191222/1645
Product: mt8168					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Dec-2022	6.7	In throttling, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405923; Issue ID: ALPS07405923. **CVE ID : CVE-2022-32624**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT81-191222/1646
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT81-191222/1647
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT81-191222/1648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT81-191222/1649
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT81-191222/1650
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT81-191222/1651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt8175					
Affected Version(s): -					
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT81-191222/1652
Product: mt8183					
Affected Version(s): -					
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT81-191222/1653
Product: mt8185					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT81-191222/1654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**		
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT81-191222/1655
Product: mt8321					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT83-191222/1656
Improper Input Validation	05-Dec-2022	6.7	In ccci, there is a possible out of bounds write due to improper input validation. This could	https://corp.mediatek.com/product-security-	H-MED-MT83-191222/1657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	bulletin/December-2022	
Product: mt8362a					
Affected Version(s): -					
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT83-191222/1658
Product: mt8365					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In throttling, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405923; Issue ID: ALPS07405923.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT83-191222/1659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32624		
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT83-191222/1660
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT83-191222/1661
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT83-191222/1662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32631		
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT83-191222/1663
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT83-191222/1664
Product: mt8385					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT83-191222/1665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT83-191222/1666
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT83-191222/1667
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT83-191222/1668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**		
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT83-191222/1669
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT83-191222/1670
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT83-191222/1671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**		
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT83-191222/1672
Product: mt8518					
Affected Version(s): -					
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT85-191222/1673
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT85-191222/1674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**		
Product: mt8532					
Affected Version(s): -					
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT85-191222/1675
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT85-191222/1676
Product: mt8666					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT86-191222/1677
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT86-191222/1678
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT86-191222/1679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT86-191222/1680
Product: mt8667					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT86-191222/1681
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT86-191222/1682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32631		
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT86-191222/1683
Product: mt8675					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT86-191222/1684
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT86-191222/1685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**		
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT86-191222/1686
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT86-191222/1687
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT86-191222/1688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**		
Product: mt8695					
Affected Version(s): -					
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT86-191222/1689
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT86-191222/1690
Product: mt8696					
Affected Version(s): -					
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, there is a possible out of bounds write due to improper input validation. This could lead to local	https://corp.mediatek.com/product-security-	H-MED-MT86-191222/1691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	bulletin/December-2022	
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT86-191222/1692
Product: mt8765					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1694
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1695
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1697
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1698
Product: mt8766					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32594		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1700
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1701
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32598		
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1703
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1704
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326239; Issue ID: ALPS07326239.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32626		
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1706
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1707
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32633		
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1709
Product: mt8768					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1710
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1712
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1713
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**		
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1715
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1716
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**		
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1718
Product: mt8781					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1719
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1721
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1722
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**		
Out-of-bounds Write	05-Dec-2022	6.7	In mpu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07541753; Issue ID: ALPS07541753. **CVE ID : CVE-2022-32620**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1724
Out-of-bounds Write	05-Dec-2022	6.7	In gz, there is a possible memory corruption 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. Patch ID: ALPS07363786; Issue ID: ALPS07363786. **CVE ID : CVE-2022-32622**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1725
Out-of-bounds Write	05-Dec-2022	6.7	In throttling, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405923; Issue ID: ALPS07405923. **CVE ID : CVE-2022-32624**		
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1727
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1728
Out-of-bounds Write	05-Dec-2022	6.7	In throttling, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405966; Issue ID: ALPS07405966. **CVE ID : CVE-2022-32630**		
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1730
Product: mt8786					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1731
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, there is a possible out of bounds write due to an incorrect bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT87-191222/1732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	bulletin/December-2022	
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1733
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1734
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, there is a possible out of bounds write due to an incorrect bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT87-191222/1735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	bulletin/December-2022	
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1736
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1737
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to	https://corp.mediatek.com/product-security-	H-MED-MT87-191222/1738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	bulletin/December-2022	
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1739
Product: mt8788					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1741
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1742
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1744
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1745
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1747
Product: mt8789					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1748
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32596		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1750
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1751
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32619		
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1753
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1754
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637.	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32633		
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1756
Product: mt8791					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1757
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1759
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1760
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**		
Out-of-bounds Write	05-Dec-2022	6.7	In mpu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07541753; Issue ID: ALPS07541753. **CVE ID : CVE-2022-32620**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1762
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1763
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**		
Out-of-bounds Write	05-Dec-2022	6.7	In isp, 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. Patch ID: ALPS07310780; Issue ID: ALPS07310780. **CVE ID : CVE-2022-32628**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1765
Out-of-bounds Write	05-Dec-2022	6.7	In isp, 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. Patch ID: ALPS07310774; Issue ID: ALPS07310774. **CVE ID : CVE-2022-32629**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1766
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**		
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1768
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1769
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID:	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**		
Product: mt8791t					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1771
Product: mt8797					
Affected Version(s): -					
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1772
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-	H-MED-MT87-191222/1773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	bulletin/December-2022	
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1774
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1775
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-	H-MED-MT87-191222/1776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	bulletin/December-2022	
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1777
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1778
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of	https://corp.mediatek.com/product-security-	H-MED-MT87-191222/1779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	bulletin/December-2022	
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	H-MED-MT87-191222/1780
Vendor: Medtronic					
Product: guardian_link_2_transmitter_mmt-7730					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-GUAR-191222/1781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**		
Product: guardian_link_2_transmitter_mmt-7731					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-GUAR-191222/1782
Product: guardian_link_2_transmitter_mmt-7738					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-	H-MED-GUAR-191222/1783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	communication-issue.html	
Product: guardian_link_2_transmitter_mmt-7775					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-GUAR-191222/1784
Product: guardian_link_3_transmitter_mmt-7810					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-GUAR-191222/1785
Product: guardian_link_3_transmitter_mmt-7811					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-GUAR-191222/1786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**		
Product: minimed_620g_mmt-1750					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-MINI-191222/1787
Product: minimed_630g_mmt-1715					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-MINI-191222/1788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**		
Product: minimed_630g_mmt-1754					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-MINI-191222/1789
Product: minimed_630g_mmt-1755					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the	https://global.medtronic.com/xg-en/product-	H-MED-MINI-191222/1790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	security/security-bulletins/minimed-600-series-communication-issue.html	
Product: minimed_640g_mmt-1711					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-MINI-191222/1791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: minimed_640g_mmt-1712					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-MINI-191222/1792
Product: minimed_640g_mmt-1751					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-MINI-191222/1793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**		
Product: minimed_640g_mmt-1752					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-MINI-191222/1794
Product: minimed_670g_mmt-1740					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-	H-MED-MINI-191222/1795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	communication-issue.html	
Product: minimed_670g_mmt-1741					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-MINI-191222/1796
Product: minimed_670g_mmt-1742					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an	https://global.medtronic.co	H-MED-MINI-191222/1797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	m/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	
Product: minimed_670g_mmt-1760					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-MINI-191222/1798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32537		
Product: minimed_670g_mmt-1761					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-MINI-191222/1799
Product: minimed_670g_mmt-1762					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device;	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-MINI-191222/1800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**		
Product: minimed_670g_mmt-1780					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-MINI-191222/1801
Product: minimed_670g_mmt-1781					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the	https://global.medtronic.com/xg-en/product-security/security-bulletins/mini	H-MED-MINI-191222/1802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	med-600-series-communication-issue.html	
Product: minimed_670g_mmt-1782					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-MINI-191222/1803
Product: mmt-1151					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-MMT--191222/1804
Product: mmt-1152					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-MMT--191222/1805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**		
Product: mmt-1351					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-MMT--191222/1806
Product: mmt-1352					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-MMT--191222/1807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**		
Product: mmt-7306					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	H-MED-MMT--191222/1808
Vendor: Moxa					
Product: uc-2101-lx					
Affected Version(s): -					
Improper Neutralization of	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior	N/A	H-MOX-UC-2-191222/1809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-2102-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-2-191222/1810
Product: uc-2104-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-2-191222/1811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: uc-2111-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-2-191222/1812
Product: uc-2112-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-2-191222/1813
Product: uc-2114-t-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may	N/A	H-MOX-UC-2-191222/1814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-2116-t-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-2-191222/1815
Product: uc-3101-t-ap-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-3-191222/1816
Product: uc-3101-t-eu-lx					
Affected Version(s): -					
Improper Neutralization of Special	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell	N/A	H-MOX-UC-3-191222/1817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-3101-t-us-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-3-191222/1818
Product: uc-3111-t-ap-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-3-191222/1819
Product: uc-3111-t-ap-lx-nw					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-3-191222/1820
Product: uc-3111-t-eu-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-3-191222/1821
Product: uc-3111-t-eu-lx-nw					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may	N/A	H-MOX-UC-3-191222/1822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-3111-t-us-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-3-191222/1823
Product: uc-3111-t-us-lx-nw					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-3-191222/1824
Product: uc-3121-t-ap-lx					
Affected Version(s): -					
Improper Neutralization of Special	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell	N/A	H-MOX-UC-3-191222/1825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-3121-t-eu-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-3-191222/1826
Product: uc-3121-t-us-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-3-191222/1827
Product: uc-5101-lx					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-5-191222/1828
Product: uc-5101-t-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-5-191222/1829
Product: uc-5102-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may	N/A	H-MOX-UC-5-191222/1830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-5102-t-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-5-191222/1831
Product: uc-5111-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-5-191222/1832
Product: uc-5111-t-lx					
Affected Version(s): -					
Improper Neutralization of Special	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell	N/A	H-MOX-UC-5-191222/1833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-5112-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-5-191222/1834
Product: uc-5112-t-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-5-191222/1835
Product: uc-8112-lx					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-8-191222/1836
Product: uc-8112a-me-t-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-8-191222/1837
Product: uc-8131-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may	N/A	H-MOX-UC-8-191222/1838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-8132-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-8-191222/1839
Product: uc-8162-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-8-191222/1840
Product: uc-8210-t-lx-s					
Affected Version(s): -					
Improper Neutralization of Special	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell	N/A	H-MOX-UC-8-191222/1841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-8220-t-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-8-191222/1842
Product: uc-8220-t-lx-ap-s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-8-191222/1843
Product: uc-8220-t-lx-eu-s					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-8-191222/1844
Product: uc-8220-t-lx-us-s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-8-191222/1845
Product: uc-8410a-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may	N/A	H-MOX-UC-8-191222/1846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-8410a-nw-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-8-191222/1847
Product: uc-8410a-nw-t-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-8-191222/1848
Product: uc-8410a-t-lx					
Affected Version(s): -					
Improper Neutralization of Special	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell	N/A	H-MOX-UC-8-191222/1849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-8540-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-8-191222/1850
Product: uc-8540-t-ct-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-8-191222/1851
Product: uc-8540-t-lx					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-8-191222/1852
Product: uc-8580-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-8-191222/1853
Product: uc-8580-q-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may	N/A	H-MOX-UC-8-191222/1854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-8580-t-ct-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-8-191222/1855
Product: uc-8580-t-ct-q-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-8-191222/1856
Product: uc-8580-t-lx					
Affected Version(s): -					
Improper Neutralization of Special	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell	N/A	H-MOX-UC-8-191222/1857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-8580-t-q-lx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	H-MOX-UC-8-191222/1858
Vendor: Ricoh					
Product: aficio_sp_4210n					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Dec-2022	4.8	Cross-site scripting vulnerability in Aficio SP 4210N firmware versions prior to Web Support 1.05 allows a remote authenticated attacker with an administrative privilege to inject an arbitrary script. **CVE ID : CVE-2022-37406**	https://support.ricoh.com/bb/html/dr_ut_e/rc3/model/sp42/sp42.htm, https://support.ricoh.com/bbv2/html/dr_ut_d/ipsio/history/w/bb/pub_j/dr_ut_d/4101044/4101044791/V10	H-RIC-AFIC-191222/1859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				1/5236968/redirect_CLUTool_DOM/history.htm	
Vendor: Samsung					
Product: exynos					
Affected Version(s): -					
Incorrect Authorization	08-Dec-2022	7.5	Improper authorization in Exynos baseband prior to SMR DEC-2022 Release 1 allows remote attacker to get sensitive information including IMEI via emergency call. **CVE ID : CVE-2022-39902**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	H-SAM-EXYN-191222/1860
Improper Authentication	08-Dec-2022	6.5	Improper authentication in Exynos baseband prior to SMR DEC-2022 Release 1 allows remote attacker to disable the network traffic encryption between UE and gNodeB. **CVE ID : CVE-2022-39901**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	H-SAM-EXYN-191222/1861
Vendor: secu					
Product: secustation					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	08-Dec-2022	4.9	In certain Secustation products the administrator account password can be read. This affects V2.5.5.3116-S50-SMA-B20171107A, V2.3.4.1301-M20-TSA-B20150617A, V2.5.5.3116-S50-RXA-B20180502A, V2.5.5.3116-S50-SMA-	N/A	H-SEC-SECU-191222/1862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			B20190723A, V2.5.5.3116-S50-SMB-B20161012A, V2.3.4.2103-S50-NTD-B20170508B, V2.5.5.3116-S50-SMB-B20160601A, V2.5.5.2601-S50-TSA-B20151229A, and V2.5.5.3116-S50-SMA-B20170217. **CVE ID : CVE-2022-40939**		
Vendor: Sophos					
Product: xg_firewall					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	01-Dec-2022	8.8	A code injection vulnerability allows adjacent attackers to execute code in the Wifi controller of Sophos Firewall releases older than version 19.5 GA. **CVE ID : CVE-2022-3713**	https://www.sophos.com/en-us/security-advisories/sophos-sa-20221201-sfos-19-5-0	H-SOP-XG_F-191222/1863
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-2022	8.4	A stored XSS vulnerability allows admin to super-admin privilege escalation in the Webadmin import group wizard of Sophos Firewall releases older than version 19.5 GA. **CVE ID : CVE-2022-3709**	https://www.sophos.com/en-us/security-advisories/sophos-sa-20221201-sfos-19-5-0	H-SOP-XG_F-191222/1864
Improper Neutralization of Special Elements used in an	01-Dec-2022	7.2	An OS command injection vulnerability allows admins to execute code via SSL VPN configuration uploads in Sophos Firewall releases	https://www.sophos.com/en-us/security-advisories/sophos-sa-	H-SOP-XG_F-191222/1865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			older than version 19.5 GA. **CVE ID : CVE-2022-3226**	20221201-sfos-19-5-0	
Improper Control of Generation of Code ('Code Injection')	01-Dec-2022	7.2	A post-auth code injection vulnerability allows admins to execute code in Webadmin of Sophos Firewall releases older than version 19.5 GA. **CVE ID : CVE-2022-3696**	https://www.sophos.com/en-us/security-advisories/sophos-sa-20221201-sfos-19-5-0	H-SOP-XG_F-191222/1866
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Dec-2022	4.3	A post-auth read-only SQL injection vulnerability allows users to read non-sensitive configuration database contents in the User Portal of Sophos Firewall releases older than version 19.5 GA. **CVE ID : CVE-2022-3711**	https://www.sophos.com/en-us/security-advisories/sophos-sa-20221201-sfos-19-5-0	H-SOP-XG_F-191222/1867
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Dec-2022	2.7	A post-auth read-only SQL injection vulnerability allows API clients to read non-sensitive configuration database contents in the API controller of Sophos Firewall releases older than version 19.5 GA. **CVE ID : CVE-2022-3710**	https://www.sophos.com/en-us/security-advisories/sophos-sa-20221201-sfos-19-5-0	H-SOP-XG_F-191222/1868
Vendor: telos					
Product: omnia_mpx_node					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	02-Dec-2022	8.8	Insecure permissions in Telos Alliance Omnia MPX Node v1.0.0 to v1.4.9 allow attackers to manipulate and access system settings with backdoor account low privilege, this can lead to change hardware settings and execute arbitrary commands in vulnerable system functions that is requires high privilege to access. **CVE ID : CVE-2022-45562**	N/A	H-TEL-OMNI-191222/1869
Vendor: telosalliance					
Product: omnia_mpx_node					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Dec-2022	9.8	An unauthenticated command injection vulnerability in the product license validation function of Telos Alliance Omnia MPX Node 1.3.* - 1.4.* allows attackers to execute arbitrary commands via a crafted payload injected into the license input. **CVE ID : CVE-2022-43325**	N/A	H-TEL-OMNI-191222/1870
Vendor: Tenda					
Product: a18					
Affected Version(s): -					
Out-of-bounds Write	08-Dec-2022	7.5	Tenda A18 v15.13.07.09 was discovered to contain a stack overflow via the security_5g	https://github.com/z1r00/IOT_Vul/blob/main/Tenda/A18/formWi	H-TEN-A18-191222/1871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter at /goform/WifiBasicSet. **CVE ID : CVE-2022-44931**	fiBasicSet/readme.md	
N/A	08-Dec-2022	7.5	An access control issue in Tenda A18 v15.13.07.09 allows unauthenticated attackers to access the Telnet service. **CVE ID : CVE-2022-44932**	N/A	H-TEN-A18-191222/1872
Product: ac6					
Affected Version(s): 1.0					
Out-of-bounds Write	01-Dec-2022	7.5	Tenda Tenda AC6V1.0 V15.03.05.19 is affected by buffer overflow. Causes a denial of service (local). **CVE ID : CVE-2022-45640**	N/A	H-TEN-AC6-191222/1873
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 is vulnerable to Buffer Overflow via formSetMacFilterCfg. **CVE ID : CVE-2022-45641**	N/A	H-TEN-AC6-191222/1874
Cross-Site Request Forgery (CSRF)	02-Dec-2022	6.5	Tenda AC6V1.0 V15.03.05.19 is vulnerable to Cross Site Request Forgery (CSRF) via function fromSysToolRestoreSet. **CVE ID : CVE-2022-45673**	N/A	H-TEN-AC6-191222/1875
Cross-Site Request	02-Dec-2022	6.5	Tenda AC6V1.0 V15.03.05.19 is vulnerable to Cross Site	N/A	H-TEN-AC6-191222/1876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Request Forgery (CSRF) via function fromSysToolReboot. **CVE ID : CVE-2022-45674**		
Product: ax12					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Dec-2022	8.8	Tenda AX12 V22.03.01.16_cn is vulnerable to command injection via goform/fast_setting_internet_set. **CVE ID : CVE-2022-45043**	N/A	H-TEN-AX12-191222/1877
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Dec-2022	8.8	Tenda AX12 V22.03.01.21_CN was found to have a command injection vulnerability via /goform/setMacFilterCfg function. **CVE ID : CVE-2022-45977**	N/A	H-TEN-AX12-191222/1878
Cross-Site Request Forgery (CSRF)	12-Dec-2022	8.8	Tenda AX12 V22.03.01.21_CN was discovered to contain a Cross-Site Request Forgery (CSRF) via /goform/SysToolRestoreSet . **CVE ID : CVE-2022-45980**	N/A	H-TEN-AX12-191222/1879
Out-of-bounds Write	12-Dec-2022	7.5	Tenda AX12 v22.03.01.21_CN was discovered to contain a stack overflow via the ssid parameter at	N/A	H-TEN-AX12-191222/1880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/goform/fast_setting_wifi_set . **CVE ID : CVE-2022-45979**		
Product: i21					
Affected Version(s): -					
Out-of-bounds Write	02-Dec-2022	9.8	Tenda i21 V1.0.0.14(4656) is vulnerable to Buffer Overflow via /goform/AddSysLogRule . **CVE ID : CVE-2022-44362**	N/A	H-TEN-I21-191222/1881
Out-of-bounds Write	02-Dec-2022	9.8	Tenda i21 V1.0.0.14(4656) is vulnerable to Buffer Overflow via /goform/setSnmpInfo. **CVE ID : CVE-2022-44363**	N/A	H-TEN-I21-191222/1882
Out-of-bounds Write	02-Dec-2022	9.8	Tenda i21 V1.0.0.14(4656) has a stack overflow vulnerability via /goform/setSysPwd. **CVE ID : CVE-2022-44365**	N/A	H-TEN-I21-191222/1883
Out-of-bounds Write	02-Dec-2022	9.8	Tenda i21 V1.0.0.14(4656) is vulnerable to Buffer Overflow via /goform/setDiagnoseInfo. **CVE ID : CVE-2022-44366**	N/A	H-TEN-I21-191222/1884
Out-of-bounds Write	02-Dec-2022	9.8	Tenda i21 V1.0.0.14(4656) is vulnerable to Buffer	N/A	H-TEN-I21-191222/1885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Overflow via /goform/setUplinkInfo. **CVE ID : CVE-2022-44367**		
Product: i22					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the index parameter in the formWifiMacFilterSet function. **CVE ID : CVE-2022-45663**	N/A	H-TEN-I22-191222/1886
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the list parameter in the formwrlSSIDget function. **CVE ID : CVE-2022-45664**	N/A	H-TEN-I22-191222/1887
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the index parameter in the formWifiMacFilterGet function. **CVE ID : CVE-2022-45669**	N/A	H-TEN-I22-191222/1888
Buffer Copy without Checking Size of Input ('Classic	02-Dec-2022	7.5	Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the ping1 parameter in the formSetAutoPing function.	N/A	H-TEN-I22-191222/1889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			**CVE ID : CVE-2022-45670**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the appData parameter in the formSetAppFilterRule function. **CVE ID : CVE-2022-45671**	N/A	H-TEN-I22-191222/1890
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the formWx3AuthorizeSet function. **CVE ID : CVE-2022-45672**	N/A	H-TEN-I22-191222/1891
Cross-Site Request Forgery (CSRF)	02-Dec-2022	6.5	Tenda i22 V1.0.0.3(4687) is vulnerable to Cross Site Request Forgery (CSRF) via function fromSysToolRestoreSet. **CVE ID : CVE-2022-45667**	N/A	H-TEN-I22-191222/1892
Cross-Site Request Forgery (CSRF)	02-Dec-2022	6.5	Tenda i22 V1.0.0.3(4687) is vulnerable to Cross Site Request Forgery (CSRF) via function fromSysToolReboot. **CVE ID : CVE-2022-45668**	N/A	H-TEN-I22-191222/1893
Product: w15e					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Dec-2022	7.2	Tenda W20E V16.01.0.6(3392) is vulnerable to Command injection via cmd_get_ping_output. **CVE ID : CVE-2022-45996**	N/A	H-TEN-W15E-191222/1894
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Dec-2022	7.2	Tenda W20E V16.01.0.6(3392) is vulnerable to Buffer Overflow. **CVE ID : CVE-2022-45997**	N/A	H-TEN-W15E-191222/1895
Product: w30e					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Dec-2022	9.8	Tenda W30E v1.0.1.25(633) was discovered to contain a command injection vulnerability via the fileNameMit parameter at /goform/delFileName. **CVE ID : CVE-2022-45506**	N/A	H-TEN-W30E-191222/1896
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the cmdinput parameter at /goform/exeCommand. **CVE ID : CVE-2022-45505**	N/A	H-TEN-W30E-191222/1897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the editNameMit parameter at /goform/editFileName. **CVE ID : CVE-2022-45507**	N/A	H-TEN-W30E-191222/1898
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the new_account parameter at /goform/editUserName. **CVE ID : CVE-2022-45508**	N/A	H-TEN-W30E-191222/1899
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the account parameter at /goform/addUserName. **CVE ID : CVE-2022-45509**	N/A	H-TEN-W30E-191222/1900
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the mit_ssid_index parameter at /goform/AdvSetWrlsafeset. **CVE ID : CVE-2022-45510**	N/A	H-TEN-W30E-191222/1901
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the PPPOEPassword	N/A	H-TEN-W30E-191222/1902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter at /goform/QuickIndex. **CVE ID : CVE-2022-45511**		
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/SafeEmailFilter. **CVE ID : CVE-2022-45512**	N/A	H-TEN-W30E-191222/1903
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/P2pListFilter. **CVE ID : CVE-2022-45513**	N/A	H-TEN-W30E-191222/1904
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/webExcptypemanFilter. **CVE ID : CVE-2022-45514**	N/A	H-TEN-W30E-191222/1905
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the entries parameter at /goform/addressNat. **CVE ID : CVE-2022-45515**	N/A	H-TEN-W30E-191222/1906
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the	N/A	H-TEN-W30E-191222/1907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page parameter at /goform/NatStaticSettin g. **CVE ID : CVE-2022-45516**		
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/VirtualSer. **CVE ID : CVE-2022-45517**	N/A	H-TEN-W30E-191222/1908
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/SetIpBind. **CVE ID : CVE-2022-45518**	N/A	H-TEN-W30E-191222/1909
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the Go parameter at /goform/SafeMacFilter. **CVE ID : CVE-2022-45519**	N/A	H-TEN-W30E-191222/1910
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/qossetting. **CVE ID : CVE-2022-45520**	N/A	H-TEN-W30E-191222/1911
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the	N/A	H-TEN-W30E-191222/1912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page parameter at /goform/SafeUrlFilter. **CVE ID : CVE-2022-45521**		
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/SafeClientFilter. **CVE ID : CVE-2022-45522**	N/A	H-TEN-W30E-191222/1913
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/L7Im. **CVE ID : CVE-2022-45523**	N/A	H-TEN-W30E-191222/1914
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the opttype parameter at /goform/IPSECsave. **CVE ID : CVE-2022-45524**	N/A	H-TEN-W30E-191222/1915
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the downaction parameter at /goform/CertListInfo. **CVE ID : CVE-2022-45525**	N/A	H-TEN-W30E-191222/1916
Product: w6-s					
Affected Version(s): -					
Improper Neutralizat	08-Dec-2022	9.8	Tenda W6-S v1.0.0.4(510) was	N/A	H-TEN-W6-S-191222/1917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			discovered to contain a command injection vulnerability in the tpi_get_ping_output function at /goform/exeCommand. **CVE ID : CVE-2022-45497**		
N/A	08-Dec-2022	7.5	An issue in the component tpi_systool_handle(0) (/goform/SysToolReboot) of Tenda W6-S v1.0.0.4(510) allows unauthenticated attackers to arbitrarily reboot the device. **CVE ID : CVE-2022-45498**	N/A	H-TEN-W6-S-191222/1918
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W6-S v1.0.0.4(510) was discovered to contain a stack overflow via the wl_radio parameter at /goform/WifiMacFilterGet. **CVE ID : CVE-2022-45499**	N/A	H-TEN-W6-S-191222/1919
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W6-S v1.0.0.4(510) was discovered to contain a stack overflow via the wl_radio parameter at /goform/wifiSSIDset. **CVE ID : CVE-2022-45501**	N/A	H-TEN-W6-S-191222/1920
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W6-S v1.0.0.4(510) was discovered to contain a stack overflow via the	N/A	H-TEN-W6-S-191222/1921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			linkEn parameter at /goform/setAutoPing. **CVE ID : CVE-2022-45503**		
N/A	08-Dec-2022	7.5	An issue in the component tpi_systool_handle(0) (/goform/SysToolRestoreSet) of Tenda W6-S v1.0.0.4(510) allows unauthenticated attackers to arbitrarily reboot the device. **CVE ID : CVE-2022-45504**	N/A	H-TEN-W6-S-191222/1922
Vendor: Tendacn					
Product: ac6					
Affected Version(s): 1.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the deviceId parameter in the addWifiMacFilter function. **CVE ID : CVE-2022-45643**	N/A	H-TEN-AC6-191222/1923
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2022-45644**	N/A	H-TEN-AC6-191222/1924
Buffer Copy without Checking	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the	N/A	H-TEN-AC6-191222/1925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			deviceMac parameter in the addWifiMacFilter function. **CVE ID : CVE-2022-45645**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the limitSpeedUp parameter in the formSetClientState function. **CVE ID : CVE-2022-45646**	N/A	H-TEN-AC6-191222/1926
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the limitSpeed parameter in the formSetClientState function. **CVE ID : CVE-2022-45647**	N/A	H-TEN-AC6-191222/1927
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the devName parameter in the formSetDeviceName function. **CVE ID : CVE-2022-45648**	N/A	H-TEN-AC6-191222/1928
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the endIp parameter in the formSetPPTPServer function. **CVE ID : CVE-2022-45649**	N/A	H-TEN-AC6-191222/1929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the firewallEn parameter in the formSetFirewallCfg function. **CVE ID : CVE-2022-45650**	N/A	H-TEN-AC6-191222/1930
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the list parameter in the formSetVirtualSer function. **CVE ID : CVE-2022-45651**	N/A	H-TEN-AC6-191222/1931
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the startIp parameter in the formSetPPTPServer function. **CVE ID : CVE-2022-45652**	N/A	H-TEN-AC6-191222/1932
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the page parameter in the fromNatStaticSetting function. **CVE ID : CVE-2022-45653**	N/A	H-TEN-AC6-191222/1933
Buffer Copy without Checking Size of	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the ssid parameter in the	N/A	H-TEN-AC6-191222/1934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			form_fast_setting_wifi_set function. **CVE ID : CVE-2022-45654**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the timeZone parameter in the form_fast_setting_wifi_set function. **CVE ID : CVE-2022-45655**	N/A	H-TEN-AC6-191222/1935
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the time parameter in the fromSetSysTime function. **CVE ID : CVE-2022-45656**	N/A	H-TEN-AC6-191222/1936
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the list parameter in the fromSetIpMacBind function. **CVE ID : CVE-2022-45657**	N/A	H-TEN-AC6-191222/1937
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the schedEndTime parameter in the setSchedWifi function. **CVE ID : CVE-2022-45658**	N/A	H-TEN-AC6-191222/1938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the wpapsk_crypto parameter in the fromSetWirelessRepeat function. **CVE ID : CVE-2022-45659**	N/A	H-TEN-AC6-191222/1939
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the schedStartTime parameter in the setSchedWifi function. **CVE ID : CVE-2022-45660**	N/A	H-TEN-AC6-191222/1940
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the time parameter in the setSmartPowerManagement function. **CVE ID : CVE-2022-45661**	N/A	H-TEN-AC6-191222/1941
Vendor: Tp-link					
Product: re3000					
Affected Version(s): 1.0					
Improper Input Validation	07-Dec-2022	5.5	tdpServer of TP-Link RE300 V1 improperly processes its input, which may allow an attacker to cause a denial-of-service (DoS) condition of the product's OneMesh function.	https://www.tp-link.com/en/support/download/re300/v1/#Firmware	H-TP--RE30-191222/1942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41783		
Product: tl-wr740n					
Affected Version(s): -					
Improper Resource Shutdown or Release	06-Dec-2022	5.5	A vulnerability classified as problematic has been found in TP-Link TL-WR740N. Affected is an unknown function of the component ARP Handler. The manipulation leads to resource consumption. The attack needs to be done within the local network. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-214812. **CVE ID : CVE-2022-4296**	N/A	H-TP--TL-W-191222/1943
Vendor: Trendnet					
Product: tew-820ap					
Affected Version(s): 1.0r					
Out-of-bounds Write	07-Dec-2022	8.8	A stack overflow vulnerability exists in TrendNet Wireless AC Easy-Upgrader TEW-820AP (Version v1.0R, firmware version 1.01.B01) which may result in remote code execution. **CVE ID : CVE-2022-44373**	N/A	H-TRE-TEW--191222/1944
Vendor: ui					
Product: edgemax_edgerouter					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Dec-2022	8.8	A remote code execution vulnerability in EdgeRouters (Version 2.0.9-hotfix.4 and earlier) allows a malicious actor with an operator account to run arbitrary administrator commands.This vulnerability is fixed in Version 2.0.9-hotfix.5 and later. **CVE ID : CVE-2022-43553**	https://community.ui.com/releases/Security-Advisory-Bulletin-026-026/07697c65-30b3-4c06-a158-35e06534480d	H-UI-EDGE-191222/1945
Vendor: unimo					
Product: udr-ja1604					
Affected Version(s): -					
N/A	07-Dec-2022	8.8	Hidden functionality vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings. **CVE ID : CVE-2022-43464**	http://www.unimo.co.jp/table_notice/index.php?act=1&resid=1666831567-004418	H-UNI-UDR--191222/1946
Improper Neutralization of Special Elements used in an OS Command ('OS	07-Dec-2022	8.8	OS command injection vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device	http://www.unimo.co.jp/table_notice/index.php?act=1&resid=1666831567-004418	H-UNI-UDR--191222/1947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			or alter the device settings. **CVE ID : CVE-2022-44606**		
Improper Authentication	07-Dec-2022	8.8	Improper authentication vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings. **CVE ID : CVE-2022-44620**	http://www.unimo.co.jp/table_notice/index.php?act=1&resid=1666831567-004418	H-UNI-UDR--191222/1948
Product: udr-ja1608					
Affected Version(s): -					
N/A	07-Dec-2022	8.8	Hidden functionality vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings. **CVE ID : CVE-2022-43464**	http://www.unimo.co.jp/table_notice/index.php?act=1&resid=1666831567-004418	H-UNI-UDR--191222/1949
Improper Neutralization of Special Elements used in an OS	07-Dec-2022	8.8	OS command injection vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote	http://www.unimo.co.jp/table_notice/index.php?act=1&resid=1666831567-004418	H-UNI-UDR--191222/1950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			authenticated attacker to execute an arbitrary OS command on the device or alter the device settings. **CVE ID : CVE-2022-44606**		
Improper Authentication	07-Dec-2022	8.8	Improper authentication vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings. **CVE ID : CVE-2022-44620**	http://www.unimo.co.jp/table_notice/index.php?act=1&resid=1666831567-004418	H-UNI-UDR--191222/1951
Product: udr-ja1616					
Affected Version(s): -					
N/A	07-Dec-2022	8.8	Hidden functionality vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings. **CVE ID : CVE-2022-43464**	http://www.unimo.co.jp/table_notice/index.php?act=1&resid=1666831567-004418	H-UNI-UDR--191222/1952
Improper Neutralization of Special	07-Dec-2022	8.8	OS command injection vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616	http://www.unimo.co.jp/table_notice/index.php?act=	H-UNI-UDR--191222/1953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings. **CVE ID : CVE-2022-44606**	1&resid=1666831567-004418	
Improper Authentication	07-Dec-2022	8.8	Improper authentication vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings. **CVE ID : CVE-2022-44620**	http://www.unimo.co.jp/table_notice/index.php?act=1&resid=1666831567-004418	H-UNI-UDR--191222/1954
Vendor: unisoc					
Product: s8000					
Affected Version(s): -					
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39090**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1955
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up	https://www.unisoc.com/en_us/secy/announcementD	H-UNI-S800-191222/1956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39091**	etail/15995880609884110 06	
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39092**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1957
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39093**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1958
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39094**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1959
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-S800-191222/1960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service with no additional execution privileges needed. **CVE ID : CVE-2022-39095**	8060988411006	
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39096**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1961
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39097**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1962
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39098**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1963
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-S800-191222/1964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. **CVE ID : CVE-2022-39099**	806098841106	
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39100**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1965
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39101**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1966
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39102**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1967
Missing Authorization	06-Dec-2022	7.8	In UscAIEngine service, there is a missing permission check. This could lead to set up UscAIEngine service with no additional execution privileges needed.	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42776		
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-42777**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-S800-191222/1969
Missing Authorization	06-Dec-2022	7.8	In windows manager service, there is a missing permission check. This could lead to set up windows manager service with no additional execution privileges needed. **CVE ID : CVE-2022-42778**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-S800-191222/1970
Out-of-bounds Write	06-Dec-2022	5.5	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39106**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-S800-191222/1971
Out-of-bounds Write	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39129**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-S800-191222/1972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39130**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1973
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39131**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1974
Out-of-bounds Write	06-Dec-2022	5.5	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39132**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1975
Use After Free	06-Dec-2022	5.5	In npu driver, there is a memory corruption due to a use after free. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42754**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1976
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In sensor driver, there is a possible buffer overflow due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42756**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42761**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1978
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42765**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1979
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42775**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1980
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42782**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1981
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In audio driver, there is a use after free due to a race condition. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39134**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1982
Product: s8001					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42773**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1983
Product: s8002					
Affected Version(s): -					
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42774**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1984
Product: s8003					
Affected Version(s): -					
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42779**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1985
Product: s8005					
Affected Version(s): -					
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42780**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1986
Product: s8006					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42781**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1987
Product: s8007					
Affected Version(s): -					
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42762**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1988
Product: s8008					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42763**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1989
Product: s8009					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42764**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S800-191222/1990
Product: s8010					
Affected Version(s): -					
Integer Overflow	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds	https://www.unisoc.com/e	H-UNI-S801-191222/1991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42765**	n_us/secy/announcementDetail/15995880609884110 06	
Product: s8011					
Affected Version(s): -					
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42766**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S801-191222/1992
Product: s8012					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42767**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S801-191222/1993
Product: s8013					
Affected Version(s): -					
Out-of-bounds Read	06-Dec-2022	4.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42768**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S801-191222/1994
Product: s8014					
Affected Version(s): -					
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to	https://www.unisoc.com/en_us/secy/announcementD	H-UNI-S801-191222/1995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local denial of service in wlan services. **CVE ID : CVE-2022-42769**	etail/159958806098841106	
Product: s8015					
Affected Version(s): -					
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42757**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S801-191222/1996
Product: s8016					
Affected Version(s): -					
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42758**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S801-191222/1997
Product: s8017					
Affected Version(s): -					
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42759**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S801-191222/1998
Product: s8018					
Affected Version(s): -					
Buffer Copy without Checking Size of	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-S801-191222/1999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			**CVE ID : CVE-2022-42760**	8060988411006	
Product: s8019					
Affected Version(s): -					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42770**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S801-191222/2000
Product: s8020					
Affected Version(s): -					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42771**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S802-191222/2001
Product: s8021					
Affected Version(s): -					
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42772**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S802-191222/2002
Product: s8022					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-39133**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S802-191222/2003
Product: s8023					
Affected Version(s): -					
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42755**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-S802-191222/2004
Product: sc7731e					
Affected Version(s): -					
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39090**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2005
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39091**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39092**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2007
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39093**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2008
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39094**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2009
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39095**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39096**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2011
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39097**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2012
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39098**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2013
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39099**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39100**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2015
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39101**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2016
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39102**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2017
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-42777**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In UscAIEngine service, there is a missing permission check. This could lead to set up UscAIEngine service with no additional execution privileges needed. **CVE ID : CVE-2022-42776**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2019
Missing Authorization	06-Dec-2022	7.8	In windows manager service, there is a missing permission check. This could lead to set up windows manager service with no additional execution privileges needed. **CVE ID : CVE-2022-42778**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2020
Out-of-bounds Write	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39129**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2021
Out-of-bounds Read	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39130**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2022
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This	https://www.unisoc.com/en_us/secy/announcementD	H-UNI-SC77-191222/2023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service in kernel. **CVE ID : CVE-2022-39131**	etail/159958806098841100 6	
Out-of-bounds Write	06-Dec-2022	5.5	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39132**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2024
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-39133**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2025
Use After Free	06-Dec-2022	5.5	In npu driver, there is a memory corruption due to a use after free. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42754**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2026
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42755**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2027
Buffer Copy without Checking Size of Input ('Classic	06-Dec-2022	5.5	In sensor driver, there is a possible buffer overflow due to a missing bounds check. This could lead to local denial of service in kernel.	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			**CVE ID : CVE-2022-42756**		
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42764**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2029
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42759**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2030
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42760**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2031
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42761**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2032
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42762**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42763**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2034
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42765**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2035
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42766**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2036
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42772**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2037
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42773**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2038
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-SC77-191222/2039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42774	8060988411006	
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42775**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2040
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42782**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2041
Out-of-bounds Write	06-Dec-2022	5.5	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39106**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2042
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42779**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2043
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42780**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42781**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2045
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In audio driver, there is a use after free due to a race condition. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39134**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2046
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42771**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2047
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42770**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC77-191222/2048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	4.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42768**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2049
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42769**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2050
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42757**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2051
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42758**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2052
Integer Overflow or Wraparound	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42767**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC77-191222/2053
Product: sc9832e					
Affected Version(s): -					
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This	https://www.unisoc.com/en_us/secy/an	H-UNI-SC98-191222/2054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39090**	nouncementDetail/15995880609884110 06	
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39091**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2055
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39092**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2056
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39093**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2057
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up	https://www.unisoc.com/en_us/secy/announcementD	H-UNI-SC98-191222/2058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39094**	etail/15995880609884110 06	
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39095**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2059
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39096**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2060
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39097**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2061
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-SC98-191222/2062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service with no additional execution privileges needed. **CVE ID : CVE-2022-39098**	8060988411006	
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39099**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2063
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39100**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2064
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39101**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2065
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-SC98-191222/2066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. **CVE ID : CVE-2022-39102**	8060988411006	
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-42777**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2067
Missing Authorization	06-Dec-2022	7.8	In UscAIEngine service, there is a missing permission check. This could lead to set up UscAIEngine service with no additional execution privileges needed. **CVE ID : CVE-2022-42776**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2068
Missing Authorization	06-Dec-2022	7.8	In windows manager service, there is a missing permission check. This could lead to set up windows manager service with no additional execution privileges needed. **CVE ID : CVE-2022-42778**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2069
Out-of-bounds Write	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39129		
Out-of-bounds Read	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39130**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2071
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39131**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2072
Out-of-bounds Write	06-Dec-2022	5.5	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39132**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2073
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-39133**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2074
Use After Free	06-Dec-2022	5.5	In npu driver, there is a memory corruption due to a use after free. This could lead to local denial of service in kernel.	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42754		
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42755**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC98-191222/2076
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In sensor driver, there is a possible buffer overflow due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42756**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC98-191222/2077
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42764**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC98-191222/2078
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42759**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC98-191222/2079
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42760**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC98-191222/2080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42761**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2081
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42762**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2082
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42763**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2083
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42765**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2084
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42766**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2085
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-SC98-191222/2086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42772	8060988411006	
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42773**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2087
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42774**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2088
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42775**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2089
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42782**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2090
Out-of-bounds Write	06-Dec-2022	5.5	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39106**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42779**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2092
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42780**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2093
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42781**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2094
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In audio driver, there is a use after free due to a race condition. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39134**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2095
Concurrent Execution using Shared Resource with Improper Synchronization	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42771**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42770**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2097
Out-of-bounds Read	06-Dec-2022	4.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42768**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2098
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42769**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2099
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42757**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2100
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42758**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42767**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2102
Product: sc9863a					
Affected Version(s): -					
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39090**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2103
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39091**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2104
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39092**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39093**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC98-191222/2106
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39094**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC98-191222/2107
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39095**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC98-191222/2108
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39096**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC98-191222/2109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39097**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC98-191222/2110
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39098**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC98-191222/2111
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39099**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC98-191222/2112
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39100**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC98-191222/2113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39101**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2114
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39102**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2115
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-42777**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2116
Missing Authorization	06-Dec-2022	7.8	In UscAIEngine service, there is a missing permission check. This could lead to set up UscAIEngine service with no additional execution privileges needed. **CVE ID : CVE-2022-42776**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In windows manager service, there is a missing permission check. This could lead to set up windows manager service with no additional execution privileges needed. **CVE ID : CVE-2022-42778**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2118
Out-of-bounds Write	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39129**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2119
Out-of-bounds Read	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39130**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2120
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39131**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2121
Out-of-bounds Write	06-Dec-2022	5.5	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-SC98-191222/2122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local denial of service in kernel. **CVE ID : CVE-2022-39132**	8060988411006	
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-39133**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2123
Use After Free	06-Dec-2022	5.5	In npu driver, there is a memory corruption due to a use after free. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42754**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2124
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42755**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2125
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In sensor driver, there is a possible buffer overflow due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42756**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2126
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-SC98-191222/2127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42764	8060988411006	
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42759**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2128
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42760**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2129
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42761**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2130
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42762**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2131
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42763**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42765**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2133
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42766**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2134
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42772**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2135
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42773**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2136
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42774**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2137
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-SC98-191222/2138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service in kernel. **CVE ID : CVE-2022-42775**	806098841100 6	
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42782**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2139
Out-of-bounds Write	06-Dec-2022	5.5	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39106**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2140
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42779**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2141
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42780**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2142
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42781**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In audio driver, there is a use after free due to a race condition. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39134**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2144
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42771**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2145
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42770**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2146
Out-of-bounds Read	06-Dec-2022	4.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42768**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-SC98-191222/2147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42769**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC98-191222/2148
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42757**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC98-191222/2149
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42758**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC98-191222/2150
Integer Overflow or Wraparound	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42767**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-SC98-191222/2151
Product: t310					
Affected Version(s): -					
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39090**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T310-191222/2152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39091**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2153
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39092**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2154
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39093**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2155
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39094**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39095**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T310-191222/2157
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39096**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T310-191222/2158
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39097**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T310-191222/2159
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39098**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T310-191222/2160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39099**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T310-191222/2161
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39100**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T310-191222/2162
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39101**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T310-191222/2163
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39102**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T310-191222/2164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-42777**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T310-191222/2165
Missing Authorization	06-Dec-2022	7.8	In UscAIEngine service, there is a missing permission check. This could lead to set up UscAIEngine service with no additional execution privileges needed. **CVE ID : CVE-2022-42776**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T310-191222/2166
Missing Authorization	06-Dec-2022	7.8	In windows manager service, there is a missing permission check. This could lead to set up windows manager service with no additional execution privileges needed. **CVE ID : CVE-2022-42778**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T310-191222/2167
Out-of-bounds Write	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39129**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T310-191222/2168
Out-of-bounds Read	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a	https://www.unisoc.com/en_us/secy/an	H-UNI-T310-191222/2169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39130**	nouncementDetail/15995880609884110 06	
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39131**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2170
Out-of-bounds Write	06-Dec-2022	5.5	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39132**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2171
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-39133**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2172
Use After Free	06-Dec-2022	5.5	In npu driver, there is a memory corruption due to a use after free. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42754**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2173
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T310-191222/2174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local denial of service in wlan services. **CVE ID : CVE-2022-42755**	8060988411006	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In sensor driver, there is a possible buffer overflow due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42756**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2175
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42764**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2176
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42759**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2177
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42760**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2178
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T310-191222/2179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42761	8060988411006	
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42762**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2180
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42763**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2181
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42765**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2182
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42766**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2183
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42772**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2184
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to	https://www.unisoc.com/en_us/secy/an	H-UNI-T310-191222/2185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local denial of service in wlan services. **CVE ID : CVE-2022-42773**	nouncementDetail/15995880609884110 06	
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42774**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2186
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42775**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2187
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42782**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2188
Out-of-bounds Write	06-Dec-2022	5.5	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39106**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2189
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T310-191222/2190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42779	8060988411006	
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42780**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2191
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42781**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2192
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In audio driver, there is a use after free due to a race condition. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39134**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2193
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42771**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2194
Concurrent Execution using Shared	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial	https://www.unisoc.com/en_us/secy/announcementD	H-UNI-T310-191222/2195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			of service in wlan services. **CVE ID : CVE-2022-42770**	etail/159958806098841106	
Out-of-bounds Read	06-Dec-2022	4.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42768**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2196
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42769**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2197
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42757**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2198
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42758**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T310-191222/2199
Integer Overflow or Wraparound	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T310-191222/2200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42767	8060988411006	
Product: t606					
Affected Version(s): -					
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39090**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2201
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39091**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2202
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39092**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2203
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. **CVE ID : CVE-2022-39093**		
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39094**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T606-191222/2205
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39095**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T606-191222/2206
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39096**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T606-191222/2207
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T606-191222/2208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. **CVE ID : CVE-2022-39097**		
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39098**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T606-191222/2209
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39099**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T606-191222/2210
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39100**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T606-191222/2211
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T606-191222/2212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. **CVE ID : CVE-2022-39101**		
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39102**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T606-191222/2213
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-42777**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T606-191222/2214
Missing Authorization	06-Dec-2022	7.8	In UscAIEngine service, there is a missing permission check. This could lead to set up UscAIEngine service with no additional execution privileges needed. **CVE ID : CVE-2022-42776**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T606-191222/2215
Missing Authorization	06-Dec-2022	7.8	In windows manager service, there is a missing permission check. This could lead to set up windows manager service with no additional execution privileges needed.	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T606-191222/2216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42778		
Out-of-bounds Write	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39129**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2217
Out-of-bounds Read	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39130**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2218
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39131**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2219
Out-of-bounds Write	06-Dec-2022	5.5	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39132**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2220
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T606-191222/2221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39133	8060988411006	
Use After Free	06-Dec-2022	5.5	In npu driver, there is a memory corruption due to a use after free. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42754**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2222
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42755**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2223
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In sensor driver, there is a possible buffer overflow due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42756**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2224
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42764**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2225
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42759**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42760**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T606-191222/2227
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42761**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T606-191222/2228
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42762**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T606-191222/2229
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42763**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T606-191222/2230
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42765**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T606-191222/2231
Exposure of Resource	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This	https://www.unisoc.com/en_us/secy/announcementD	H-UNI-T606-191222/2232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			could lead to local information disclosure. **CVE ID : CVE-2022-42766**	etail/159958806098841100 6	
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42772**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2233
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42773**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2234
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42774**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2235
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42775**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2236
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42782**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Dec-2022	5.5	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39106**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2238
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42779**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2239
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42780**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2240
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42781**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2241
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In audio driver, there is a use after free due to a race condition. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39134**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42771**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2243
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42770**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2244
Out-of-bounds Read	06-Dec-2022	4.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42768**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2245
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42769**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2246
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T606-191222/2247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42757	8060988411006	
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42758**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2248
Integer Overflow or Wraparound	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42767**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T606-191222/2249
Product: t610					
Affected Version(s): -					
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39090**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2250
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39091**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39092**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T610-191222/2252
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39093**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T610-191222/2253
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39094**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T610-191222/2254
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39095**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T610-191222/2255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39096**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2256
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39097**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2257
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39098**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2258
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39099**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39100**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T610-191222/2260
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39101**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T610-191222/2261
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39102**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T610-191222/2262
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-42777**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T610-191222/2263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In UscAIEngine service, there is a missing permission check. This could lead to set up UscAIEngine service with no additional execution privileges needed. **CVE ID : CVE-2022-42776**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T610-191222/2264
Missing Authorization	06-Dec-2022	7.8	In windows manager service, there is a missing permission check. This could lead to set up windows manager service with no additional execution privileges needed. **CVE ID : CVE-2022-42778**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T610-191222/2265
Out-of-bounds Write	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39129**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T610-191222/2266
Out-of-bounds Read	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39130**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T610-191222/2267
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This	https://www.unisoc.com/en_us/secy/announcementD	H-UNI-T610-191222/2268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service in kernel. **CVE ID : CVE-2022-39131**	etail/159958806098841100 6	
Out-of-bounds Write	06-Dec-2022	5.5	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39132**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2269
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-39133**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2270
Use After Free	06-Dec-2022	5.5	In npu driver, there is a memory corruption due to a use after free. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42754**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2271
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42755**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2272
Buffer Copy without Checking Size of Input ('Classic	06-Dec-2022	5.5	In sensor driver, there is a possible buffer overflow due to a missing bounds check. This could lead to local denial of service in kernel.	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			**CVE ID : CVE-2022-42756**		
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42764**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T610-191222/2274
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42759**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T610-191222/2275
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42760**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T610-191222/2276
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42761**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T610-191222/2277
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42762**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T610-191222/2278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42763**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2279
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42765**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2280
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42766**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2281
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42772**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2282
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42773**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2283
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T610-191222/2284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42774	8060988411006	
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42775**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2285
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42782**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2286
Out-of-bounds Write	06-Dec-2022	5.5	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39106**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2287
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42779**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2288
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42780**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42781**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2290
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In audio driver, there is a use after free due to a race condition. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39134**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2291
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42771**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2292
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42770**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	4.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42768**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2294
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42769**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2295
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42757**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2296
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42758**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2297
Integer Overflow or Wraparound	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42767**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T610-191222/2298
Product: t612					
Affected Version(s): -					
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This	https://www.unisoc.com/en_us/secy/an	H-UNI-T612-191222/2299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39090**	nouncementDetail/15995880609884110 06	
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39091**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2300
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39092**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2301
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39093**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2302
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up	https://www.unisoc.com/en_us/secy/announcementD	H-UNI-T612-191222/2303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39094**	etail/15995880609884110 06	
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39095**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2304
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39096**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2305
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39097**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2306
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T612-191222/2307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service with no additional execution privileges needed. **CVE ID : CVE-2022-39098**	8060988411006	
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39099**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2308
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39100**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2309
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39101**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2310
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T612-191222/2311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. **CVE ID : CVE-2022-39102**	8060988411006	
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-42777**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2312
Missing Authorization	06-Dec-2022	7.8	In UscAIEngine service, there is a missing permission check. This could lead to set up UscAIEngine service with no additional execution privileges needed. **CVE ID : CVE-2022-42776**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2313
Missing Authorization	06-Dec-2022	7.8	In windows manager service, there is a missing permission check. This could lead to set up windows manager service with no additional execution privileges needed. **CVE ID : CVE-2022-42778**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2314
Out-of-bounds Write	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39129		
Out-of-bounds Read	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39130**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2316
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39131**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2317
Out-of-bounds Write	06-Dec-2022	5.5	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39132**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2318
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-39133**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2319
Use After Free	06-Dec-2022	5.5	In npu driver, there is a memory corruption due to a use after free. This could lead to local denial of service in kernel.	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42754		
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42755**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2321
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In sensor driver, there is a possible buffer overflow due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42756**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2322
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42764**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2323
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42759**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2324
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42760**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42761**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2326
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42762**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2327
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42763**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2328
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42765**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2329
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42766**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2330
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T612-191222/2331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42772	8060988411006	
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42773**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2332
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42774**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2333
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42775**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2334
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42782**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2335
Out-of-bounds Write	06-Dec-2022	5.5	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39106**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42779**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2337
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42780**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2338
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42781**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2339
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In audio driver, there is a use after free due to a race condition. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39134**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2340
Concurrent Execution using Shared Resource with Improper Synchronization	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42771**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42770**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2342
Out-of-bounds Read	06-Dec-2022	4.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42768**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2343
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42769**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2344
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42757**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2345
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42758**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42767**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T612-191222/2347
Product: t616					
Affected Version(s): -					
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39090**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2348
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39091**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2349
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39092**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39093**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T616-191222/2351
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39094**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T616-191222/2352
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39095**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T616-191222/2353
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39096**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T616-191222/2354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39097**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2355
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39098**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2356
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39099**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2357
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39100**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39101**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2359
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39102**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2360
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-42777**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2361
Missing Authorization	06-Dec-2022	7.8	In UscAIEngine service, there is a missing permission check. This could lead to set up UscAIEngine service with no additional execution privileges needed. **CVE ID : CVE-2022-42776**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In windows manager service, there is a missing permission check. This could lead to set up windows manager service with no additional execution privileges needed. **CVE ID : CVE-2022-42778**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T616-191222/2363
Out-of-bounds Write	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39129**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T616-191222/2364
Out-of-bounds Read	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39130**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T616-191222/2365
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39131**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T616-191222/2366
Out-of-bounds Write	06-Dec-2022	5.5	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T616-191222/2367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local denial of service in kernel. **CVE ID : CVE-2022-39132**	8060988411006	
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-39133**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2368
Use After Free	06-Dec-2022	5.5	In npu driver, there is a memory corruption due to a use after free. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42754**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2369
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42755**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2370
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In sensor driver, there is a possible buffer overflow due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42756**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2371
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T616-191222/2372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42764	8060988411006	
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42759**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2373
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42760**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2374
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42761**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2375
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42762**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2376
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42763**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42765**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2378
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42766**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2379
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42772**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2380
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42773**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2381
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42774**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2382
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T616-191222/2383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service in kernel. **CVE ID : CVE-2022-42775**	8060988411006	
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42782**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2384
Out-of-bounds Write	06-Dec-2022	5.5	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39106**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2385
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42779**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2386
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42780**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2387
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42781**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In audio driver, there is a use after free due to a race condition. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39134**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2389
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42771**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2390
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42770**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2391
Out-of-bounds Read	06-Dec-2022	4.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42768**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T616-191222/2392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42769**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T616-191222/2393
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42757**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T616-191222/2394
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42758**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T616-191222/2395
Integer Overflow or Wraparound	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42767**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T616-191222/2396
Product: t618					
Affected Version(s): -					
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39090**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T618-191222/2397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39091**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T618-191222/2398
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39092**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T618-191222/2399
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39093**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T618-191222/2400
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39094**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T618-191222/2401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39095**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T618-191222/2402
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39096**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T618-191222/2403
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39097**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T618-191222/2404
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39098**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T618-191222/2405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39099**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T618-191222/2406
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39100**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T618-191222/2407
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39101**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T618-191222/2408
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39102**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T618-191222/2409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-42777**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2410
Missing Authorization	06-Dec-2022	7.8	In UscAIEngine service, there is a missing permission check. This could lead to set up UscAIEngine service with no additional execution privileges needed. **CVE ID : CVE-2022-42776**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2411
Missing Authorization	06-Dec-2022	7.8	In windows manager service, there is a missing permission check. This could lead to set up windows manager service with no additional execution privileges needed. **CVE ID : CVE-2022-42778**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2412
Out-of-bounds Write	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39129**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2413
Out-of-bounds Read	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a	https://www.unisoc.com/en_us/secy/an	H-UNI-T618-191222/2414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39130**	nouncementDetail/15995880609884110 06	
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39131**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2415
Out-of-bounds Write	06-Dec-2022	5.5	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39132**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2416
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-39133**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2417
Use After Free	06-Dec-2022	5.5	In npu driver, there is a memory corruption due to a use after free. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42754**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2418
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T618-191222/2419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local denial of service in wlan services. **CVE ID : CVE-2022-42755**	806098841106	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In sensor driver, there is a possible buffer overflow due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42756**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2420
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42764**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2421
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42759**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2422
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42760**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2423
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T618-191222/2424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42761	8060988411006	
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42762**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2425
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42763**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2426
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42765**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2427
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42766**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2428
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42772**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2429
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to	https://www.unisoc.com/en_us/secy/an	H-UNI-T618-191222/2430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local denial of service in wlan services. **CVE ID : CVE-2022-42773**	nouncementDetail/15995880609884110 06	
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42774**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2431
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42775**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2432
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42782**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2433
Out-of-bounds Write	06-Dec-2022	5.5	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39106**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2434
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T618-191222/2435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42779	8060988411006	
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42780**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2436
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42781**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2437
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In audio driver, there is a use after free due to a race condition. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39134**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2438
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42771**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2439
Concurrent Execution using Shared	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial	https://www.unisoc.com/en_us/secy/announcementD	H-UNI-T618-191222/2440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			of service in wlan services. **CVE ID : CVE-2022-42770**	etail/159958806098841106	
Out-of-bounds Read	06-Dec-2022	4.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42768**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2441
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42769**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2442
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42757**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2443
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42758**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T618-191222/2444
Integer Overflow or Wraparound	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T618-191222/2445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42767	8060988411006	
Product: t760					
Affected Version(s): -					
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39090**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2446
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39091**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2447
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39092**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2448
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. **CVE ID : CVE-2022-39093**		
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39094**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T760-191222/2450
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39095**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T760-191222/2451
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39096**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T760-191222/2452
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T760-191222/2453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. **CVE ID : CVE-2022-39097**		
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39098**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T760-191222/2454
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39099**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T760-191222/2455
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39100**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T760-191222/2456
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T760-191222/2457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. **CVE ID : CVE-2022-39101**		
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39102**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T760-191222/2458
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-42777**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T760-191222/2459
Missing Authorization	06-Dec-2022	7.8	In UscAIEngine service, there is a missing permission check. This could lead to set up UscAIEngine service with no additional execution privileges needed. **CVE ID : CVE-2022-42776**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T760-191222/2460
Missing Authorization	06-Dec-2022	7.8	In windows manager service, there is a missing permission check. This could lead to set up windows manager service with no additional execution privileges needed.	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T760-191222/2461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42778		
Out-of-bounds Write	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39129**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2462
Out-of-bounds Read	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39130**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2463
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39131**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2464
Out-of-bounds Write	06-Dec-2022	5.5	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39132**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2465
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T760-191222/2466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39133	8060988411006	
Use After Free	06-Dec-2022	5.5	In npu driver, there is a memory corruption due to a use after free. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42754**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2467
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42755**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2468
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In sensor driver, there is a possible buffer overflow due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42756**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2469
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42764**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2470
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42759**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42760**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T760-191222/2472
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42761**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T760-191222/2473
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42762**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T760-191222/2474
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42763**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T760-191222/2475
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42765**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T760-191222/2476
Exposure of Resource	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This	https://www.unisoc.com/en_us/secy/announcementD	H-UNI-T760-191222/2477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			could lead to local information disclosure. **CVE ID : CVE-2022-42766**	etail/159958806098841100 6	
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42772**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2478
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42773**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2479
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42774**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2480
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42775**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2481
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42782**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Dec-2022	5.5	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39106**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2483
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42779**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2484
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42780**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2485
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42781**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2486
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In audio driver, there is a use after free due to a race condition. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39134**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42771**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2488
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42770**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2489
Out-of-bounds Read	06-Dec-2022	4.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42768**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2490
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42769**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2491
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T760-191222/2492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42757	8060988411006	
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42758**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2493
Integer Overflow or Wraparound	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42767**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T760-191222/2494
Product: t770					
Affected Version(s): -					
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39090**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2495
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39091**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39092**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2497
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39093**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2498
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39094**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2499
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39095**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39096**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2501
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39097**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2502
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39098**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2503
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39099**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39100**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2505
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39101**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2506
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39102**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2507
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-42777**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In UscAIEngine service, there is a missing permission check. This could lead to set up UscAIEngine service with no additional execution privileges needed. **CVE ID : CVE-2022-42776**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2509
Missing Authorization	06-Dec-2022	7.8	In windows manager service, there is a missing permission check. This could lead to set up windows manager service with no additional execution privileges needed. **CVE ID : CVE-2022-42778**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2510
Out-of-bounds Write	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39129**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2511
Out-of-bounds Read	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39130**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2512
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This	https://www.unisoc.com/en_us/secy/announcementD	H-UNI-T770-191222/2513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service in kernel. **CVE ID : CVE-2022-39131**	etail/159958806098841100 6	
Out-of-bounds Write	06-Dec-2022	5.5	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39132**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2514
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-39133**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2515
Use After Free	06-Dec-2022	5.5	In npu driver, there is a memory corruption due to a use after free. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42754**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2516
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42755**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2517
Buffer Copy without Checking Size of Input ('Classic	06-Dec-2022	5.5	In sensor driver, there is a possible buffer overflow due to a missing bounds check. This could lead to local denial of service in kernel.	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			**CVE ID : CVE-2022-42756**		
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42764**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2519
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42759**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2520
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42760**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2521
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42761**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2522
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42762**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42763**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2524
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42765**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2525
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42766**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2526
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42772**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2527
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42773**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2528
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T770-191222/2529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42774	8060988411006	
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42775**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2530
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42782**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2531
Out-of-bounds Write	06-Dec-2022	5.5	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39106**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2532
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42779**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2533
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42780**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42781**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2535
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In audio driver, there is a use after free due to a race condition. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39134**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2536
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42771**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2537
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42770**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T770-191222/2538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	4.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42768**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2539
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42769**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2540
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42757**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2541
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42758**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2542
Integer Overflow or Wraparound	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42767**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T770-191222/2543
Product: t820					
Affected Version(s): -					
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This	https://www.unisoc.com/en_us/secy/an	H-UNI-T820-191222/2544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39090**	nouncementDetail/15995880609884110 06	
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39091**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2545
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39092**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2546
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39093**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2547
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up	https://www.unisoc.com/en_us/secy/announcementD	H-UNI-T820-191222/2548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39094**	etail/15995880609884110 06	
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39095**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2549
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39096**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2550
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39097**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2551
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T820-191222/2552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service with no additional execution privileges needed. **CVE ID : CVE-2022-39098**	8060988411006	
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39099**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2553
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39100**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2554
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39101**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2555
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T820-191222/2556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. **CVE ID : CVE-2022-39102**	8060988411006	
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-42777**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2557
Missing Authorization	06-Dec-2022	7.8	In UscAIEngine service, there is a missing permission check. This could lead to set up UscAIEngine service with no additional execution privileges needed. **CVE ID : CVE-2022-42776**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2558
Missing Authorization	06-Dec-2022	7.8	In windows manager service, there is a missing permission check. This could lead to set up windows manager service with no additional execution privileges needed. **CVE ID : CVE-2022-42778**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2559
Out-of-bounds Write	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39129		
Out-of-bounds Read	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39130**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2561
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39131**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2562
Out-of-bounds Write	06-Dec-2022	5.5	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39132**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2563
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-39133**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2564
Use After Free	06-Dec-2022	5.5	In npu driver, there is a memory corruption due to a use after free. This could lead to local denial of service in kernel.	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42754		
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42755**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2566
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In sensor driver, there is a possible buffer overflow due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42756**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2567
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42764**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2568
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42759**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2569
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42760**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42761**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2571
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42762**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2572
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42763**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2573
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42765**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2574
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42766**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2575
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	H-UNI-T820-191222/2576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42772	8060988411006	
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42773**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2577
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42774**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2578
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42775**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2579
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42782**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2580
Out-of-bounds Write	06-Dec-2022	5.5	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39106**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42779**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2582
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42780**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2583
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42781**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2584
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In audio driver, there is a use after free due to a race condition. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39134**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2585
Concurrent Execution using Shared Resource with Improper Synchronization	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42771**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42770**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2587
Out-of-bounds Read	06-Dec-2022	4.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42768**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2588
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42769**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2589
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42757**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2590
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42758**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	H-UNI-T820-191222/2591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42767**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	H-UNI-T820-191222/2592
Vendor: westerndigital					
Product: my_cloud					
Affected Version(s): -					
Insufficiently Protected Credentials	09-Dec-2022	5.5	Insufficiently Protected Credentials vulnerability in the remote backups application on Western Digital My Cloud devices that could allow an attacker who has gained access to a relevant endpoint to use that information to access protected data. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29839**	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	H-WES-MY_C-191222/2593
Improper Authentication	09-Dec-2022	4.6	Improper Authentication vulnerability in the encrypted volumes and auto mount features of Western Digital My Cloud devices allows insecure direct access to the drive information in the case of a device reset. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux.	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	H-WES-MY_C-191222/2594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29838		
Product: my_cloud_dl2100					
Affected Version(s): -					
Insufficiently Protected Credentials	09-Dec-2022	5.5	Insufficiently Protected Credentials vulnerability in the remote backups application on Western Digital My Cloud devices that could allow an attacker who has gained access to a relevant endpoint to use that information to access protected data. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29839**	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	H-WES-MY_C-191222/2595
Improper Authentication	09-Dec-2022	4.6	Improper Authentication vulnerability in the encrypted volumes and auto mount features of Western Digital My Cloud devices allows insecure direct access to the drive information in the case of a device reset. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29838**	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	H-WES-MY_C-191222/2596
Product: my_cloud_dl4100					
Affected Version(s): -					
Insufficiently	09-Dec-2022	5.5	Insufficiently Protected Credentials vulnerability in the remote backups	https://www.westerndigital.com/support	H-WES-MY_C-191222/2597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			application on Western Digital My Cloud devices that could allow an attacker who has gained access to a relevant endpoint to use that information to access protected data. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29839**	/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	
Improper Authentication	09-Dec-2022	4.6	Improper Authentication vulnerability in the encrypted volumes and auto mount features of Western Digital My Cloud devices allows insecure direct access to the drive information in the case of a device reset. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29838**	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	H-WES-MY_C-191222/2598
Product: my_cloud_ex2100					
Affected Version(s): -					
Insufficiently Protected Credentials	09-Dec-2022	5.5	Insufficiently Protected Credentials vulnerability in the remote backups application on Western Digital My Cloud devices that could allow an attacker who has gained access to a relevant endpoint to use that information to access protected data. This	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	H-WES-MY_C-191222/2599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29839**		
Improper Authentication	09-Dec-2022	4.6	Improper Authentication vulnerability in the encrypted volumes and auto mount features of Western Digital My Cloud devices allows insecure direct access to the drive information in the case of a device reset. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29838**	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	H-WES-MY_C-191222/2600
Product: my_cloud_ex2_ultra					
Affected Version(s): -					
Insufficiently Protected Credentials	09-Dec-2022	5.5	Insufficiently Protected Credentials vulnerability in the remote backups application on Western Digital My Cloud devices that could allow an attacker who has gained access to a relevant endpoint to use that information to access protected data. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29839**	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	H-WES-MY_C-191222/2601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	09-Dec-2022	4.6	Improper Authentication vulnerability in the encrypted volumes and auto mount features of Western Digital My Cloud devices allows insecure direct access to the drive information in the case of a device reset. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29838**	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	H-WES-MY_C-191222/2602
Product: my_cloud_ex4100					
Affected Version(s): -					
Insufficiently Protected Credentials	09-Dec-2022	5.5	Insufficiently Protected Credentials vulnerability in the remote backups application on Western Digital My Cloud devices that could allow an attacker who has gained access to a relevant endpoint to use that information to access protected data. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29839**	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	H-WES-MY_C-191222/2603
Improper Authentication	09-Dec-2022	4.6	Improper Authentication vulnerability in the encrypted volumes and auto mount features of Western Digital My Cloud devices allows insecure direct access to the drive information in the case of	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-	H-WES-MY_C-191222/2604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a device reset. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29838**	version-5-25-124	
Product: my_cloud_home					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Dec-2022	7.8	A path traversal vulnerability was addressed in Western Digital My Cloud Home, My Cloud Home Duo and SanDisk ibi which could allow an attacker to initiate installation of custom ZIP packages and overwrite system files. This could potentially lead to a code execution. **CVE ID : CVE-2022-29837**	https://www.westerndigital.com/support/product-security/wdc-22018-western-digital-my-cloud-home-my-cloud-home-duo-and-sandisk-ibi-firmware-version-8-12-0-178	H-WES-MY_C-191222/2605
Product: my_cloud_home_duo					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Dec-2022	7.8	A path traversal vulnerability was addressed in Western Digital My Cloud Home, My Cloud Home Duo and SanDisk ibi which could allow an attacker to initiate installation of custom ZIP packages and overwrite system files. This could potentially lead to a code execution. **CVE ID : CVE-2022-29837**	https://www.westerndigital.com/support/product-security/wdc-22018-western-digital-my-cloud-home-my-cloud-home-duo-and-sandisk-ibi-firmware-version-8-12-0-178	H-WES-MY_C-191222/2606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: my_cloud_mirror_g2					
Affected Version(s): -					
Insufficiently Protected Credentials	09-Dec-2022	5.5	Insufficiently Protected Credentials vulnerability in the remote backups application on Western Digital My Cloud devices that could allow an attacker who has gained access to a relevant endpoint to use that information to access protected data. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29839**	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	H-WES-MY_C-191222/2607
Improper Authentication	09-Dec-2022	4.6	Improper Authentication vulnerability in the encrypted volumes and auto mount features of Western Digital My Cloud devices allows insecure direct access to the drive information in the case of a device reset. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29838**	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	H-WES-MY_C-191222/2608
Product: my_cloud_pr2100					
Affected Version(s): -					
Insufficiently Protected Credentials	09-Dec-2022	5.5	Insufficiently Protected Credentials vulnerability in the remote backups application on Western Digital My Cloud devices	https://www.westerndigital.com/support/product-security/wdc-	H-WES-MY_C-191222/2609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could allow an attacker who has gained access to a relevant endpoint to use that information to access protected data. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29839**	22019-my-cloud-firmware-version-5-25-124	
Improper Authentication	09-Dec-2022	4.6	Improper Authentication vulnerability in the encrypted volumes and auto mount features of Western Digital My Cloud devices allows insecure direct access to the drive information in the case of a device reset. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29838**	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	H-WES-MY_C-191222/2610
Product: my_cloud_pr4100					
Affected Version(s): -					
Insufficiently Protected Credentials	09-Dec-2022	5.5	Insufficiently Protected Credentials vulnerability in the remote backups application on Western Digital My Cloud devices that could allow an attacker who has gained access to a relevant endpoint to use that information to access protected data. This issue affects: Western Digital My Cloud My	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	H-WES-MY_C-191222/2611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29839**		
Improper Authentication	09-Dec-2022	4.6	Improper Authentication vulnerability in the encrypted volumes and auto mount features of Western Digital My Cloud devices allows insecure direct access to the drive information in the case of a device reset. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29838**	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	H-WES-MY_C-191222/2612
Product: sandisk_ibi					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Dec-2022	7.8	A path traversal vulnerability was addressed in Western Digital My Cloud Home, My Cloud Home Duo and SanDisk ibi which could allow an attacker to initiate installation of custom ZIP packages and overwrite system files. This could potentially lead to a code execution. **CVE ID : CVE-2022-29837**	https://www.westerndigital.com/support/product-security/wdc-22018-western-digital-my-cloud-home-my-cloud-home-duo-and-sandisk-ibi-firmware-version-8-12-0-178	H-WES-SAND-191222/2613
Product: wd_cloud					
Affected Version(s): -					
Insufficiently	09-Dec-2022	5.5	Insufficiently Protected Credentials vulnerability in the remote backups	https://www.westerndigital.com/support	H-WES-WD_C-191222/2614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			application on Western Digital My Cloud devices that could allow an attacker who has gained access to a relevant endpoint to use that information to access protected data. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29839**	/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	
Improper Authentication	09-Dec-2022	4.6	Improper Authentication vulnerability in the encrypted volumes and auto mount features of Western Digital My Cloud devices allows insecure direct access to the drive information in the case of a device reset. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29838**	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	H-WES-WD_C-191222/2615
Vendor: xiongmaitech					
Product: mbd6304t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute	N/A	H-XIO-MBD6-191222/2616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd6808t-pl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect	N/A	H-XIO-NBD6-191222/2617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7004t-p					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from	N/A	H-XIO-NBD7-191222/2618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD7-191222/2619
Product: nbd7008t-p					
Affected Version(s): -					
Improper Neutralization of	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T	N/A	H-XIO-NBD7-191222/2620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	H-XIO-NBD7-191222/2621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7016t-f-v2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	H-XIO-NBD7-191222/2622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	H-XIO-NBD7-191222/2623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd7024h-p					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD7-191222/2624
Affected Version(s): *					
Improper Neutralization of Special Elements	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and	N/A	H-XIO-NBD7-191222/2625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7024t-p					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A	N/A	H-XIO-NBD7-191222/2626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an	N/A	H-XIO-NBD7-191222/2627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7804r-fw					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD7-191222/2628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD7-191222/2629
Product: nbd7804r-f\(ep\)					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12	N/A	H-XIO-NBD7-191222/2630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default	N/A	H-XIO-NBD7-191222/2631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7804r-f\(hdmi\)					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has	N/A	H-XIO-NBD7-191222/2632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD7-191222/2633
Product: nbd7804t-pl					
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')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD7-191222/2634
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute	N/A	H-XIO-NBD7-191222/2635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7808r-pl\(ep\)					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect	N/A	H-XIO-NBD7-191222/2636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from	N/A	H-XIO-NBD7-191222/2637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7808r-pl\(hdmi\)					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD7-191222/2638
Affected Version(s): *					
Improper Neutralization of	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T	N/A	H-XIO-NBD7-191222/2639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7808t-pl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the	N/A	H-XIO-NBD7-191222/2640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	H-XIO-NBD7-191222/2641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7904r-fs					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	H-XIO-NBD7-191222/2642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD7-191222/2643
Product: nbd7904t-p					
Affected Version(s): -					
Improper Neutralization of Special Elements	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and	N/A	H-XIO-NBD7-191222/2644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and	N/A	H-XIO-NBD7-191222/2645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7904t-pl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an	N/A	H-XIO-NBD7-191222/2646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD7-191222/2647
Product: nbd7904t-pl-xpoe					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD7-191222/2648
Product: nbd7904t-plc-xpoe					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12	N/A	H-XIO-NBD7-191222/2649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7904t-q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker,	N/A	H-XIO-NBD7-191222/2650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has	N/A	H-XIO-NBD7-191222/2651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7908t-q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD7-191222/2652
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')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD7-191222/2653
Product: nbd8004r-pl\(ep\)					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated	N/A	H-XIO-NBD8-191222/2654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect	N/A	H-XIO-NBD8-191222/2655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8004r-yl\(ep\)					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from	N/A	H-XIO-NBD8-191222/2656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8004t-q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD8-191222/2657
Affected Version(s): *					
Improper Neutralization of	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T	N/A	H-XIO-NBD8-191222/2658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8008r-pl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the	N/A	H-XIO-NBD8-191222/2659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	H-XIO-NBD8-191222/2660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8008r-pl\(ep\)					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	H-XIO-NBD8-191222/2661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD8-191222/2662
Product: nbd8008r-yl\(ep\)					
Affected Version(s): -					
Improper Neutralization of Special Elements	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and	N/A	H-XIO-NBD8-191222/2663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8008ra-gl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A	N/A	H-XIO-NBD8-191222/2664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8008ra-glk					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted	N/A	H-XIO-NBD8-191222/2665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8008ra-ula					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	H-XIO-NBD8-191222/2666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd8008ra-ulk					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD8-191222/2667
Product: nbd8008ra-ul\(ep\)					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	H-XIO-NBD8-191222/2668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8008t-q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	H-XIO-NBD8-191222/2669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted	N/A	H-XIO-NBD8-191222/2670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8009s-ula-v2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	H-XIO-NBD8-191222/2671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd8010s-kl-v2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD8-191222/2672
Product: nbd8016r-ul					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	H-XIO-NBD8-191222/2673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A	N/A	H-XIO-NBD8-191222/2674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8016ra-k\(ep\)					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted	N/A	H-XIO-NBD8-191222/2675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8016ra-ul					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	H-XIO-NBD8-191222/2676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd8016ra-ula					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD8-191222/2677
Product: nbd8016ra-ulk					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	H-XIO-NBD8-191222/2678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8016ra-ul\(ep\)					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	H-XIO-NBD8-191222/2679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8016s-kl-v2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	H-XIO-NBD8-191222/2680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8016s-ula-v2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	H-XIO-NBD8-191222/2681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd8016t-q-v2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD8-191222/2682
Affected Version(s): *					
Improper Neutralization of Special Elements	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and	N/A	H-XIO-NBD8-191222/2683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8025r-ul					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A	N/A	H-XIO-NBD8-191222/2684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an	N/A	H-XIO-NBD8-191222/2685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8032h4-p					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD8-191222/2686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD8-191222/2687
Product: nbd8032h4-q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12	N/A	H-XIO-NBD8-191222/2688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default	N/A	H-XIO-NBD8-191222/2689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8032h4-qe					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has	N/A	H-XIO-NBD8-191222/2690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD8-191222/2691
Product: nbd8032h4-ul					
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')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD8-191222/2692
Product: nbd8032h8-p					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated	N/A	H-XIO-NBD8-191222/2693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect	N/A	H-XIO-NBD8-191222/2694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8032h8-qe					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from	N/A	H-XIO-NBD8-191222/2695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD8-191222/2696
Product: nbd8032ra-ul-v2					
Affected Version(s): -					
Improper Neutralization of	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T	N/A	H-XIO-NBD8-191222/2697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8064h8-p					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the	N/A	H-XIO-NBD8-191222/2698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	H-XIO-NBD8-191222/2699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd80n16ra-kl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	H-XIO-NBD8-191222/2700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd80n16ra-kl\(ep\)					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD8-191222/2701
Product: nbd80s08s-kl\(ep\)					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	H-XIO-NBD8-191222/2702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd80s10s-kl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	H-XIO-NBD8-191222/2703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd80s16s-kl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	H-XIO-NBD8-191222/2704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd80s16s-kl\(ep\)					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	H-XIO-NBD8-191222/2705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd80x09ra-kl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD8-191222/2706
Product: nbd80x09s-kl					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	H-XIO-NBD8-191222/2707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd88x09s-kl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	H-XIO-NBD8-191222/2708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8904r-pl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	H-XIO-NBD8-191222/2709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	H-XIO-NBD8-191222/2710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd8904r-yl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD8-191222/2711
Product: nbd8904t-gsc-xpoe					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	H-XIO-NBD8-191222/2712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8904t-q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	H-XIO-NBD8-191222/2713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted	N/A	H-XIO-NBD8-191222/2714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8908r-pl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	H-XIO-NBD8-191222/2715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD8-191222/2716
Product: nbd8908r-yl					
Affected Version(s): -					
Improper Neutralization of Special Elements	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and	N/A	H-XIO-NBD8-191222/2717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and	N/A	H-XIO-NBD8-191222/2718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8908t-pl-xpoe					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an	N/A	H-XIO-NBD8-191222/2719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8908t-plc-xpoe					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD8-191222/2720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nbd8916f4-q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	H-XIO-NBD8-191222/2721
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12	N/A	H-XIO-NBD8-191222/2722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8916f8-q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker,	N/A	H-XIO-NBD8-191222/2723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has	N/A	H-XIO-NBD8-191222/2724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Vendor: ZTE					
Product: otcp					
Affected Version(s): -					
Incorrect Permission Assignment for Critical Resource	05-Dec-2022	6.5	ZTE OTCP product is impacted by a permission and access control vulnerability. Due to improper permission settings, an attacker with high permissions could use this vulnerability to maliciously delete and modify files. **CVE ID : CVE-2022-23143**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026164	H-ZTE-OTCP-191222/2725
Vendor: Zyxel					
Product: atp100					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	H-ZYX-ATP1-191222/2726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**		
Product: atp100w					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	H-ZYX-ATP1-191222/2727
Product: atp200					
Affected Version(s): -					
Improper Neutralization of	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel	https://www.zyxel.com/global/en/suppo	H-ZYX-ATP2-191222/2728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	rt/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	
Product: atp500					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	H-ZYX-ATP5-191222/2729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**		
Product: atp700					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	H-ZYX-ATP7-191222/2730
Product: atp800					
Affected Version(s): -					
Improper Neutralization of Input During Web Page	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-	H-ZYX-ATP8-191222/2731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	advisory-for-xss-vulnerability-in-firewalls	
Product: usg40					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	H-ZYX-USG4-191222/2732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed on the victim's browser. **CVE ID : CVE-2022-40603**		
Product: usg40w					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	H-ZYX-USG4-191222/2733
Product: usg60					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-	H-ZYX-USG6-191222/2734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	vulnerability-in-firewalls	
Product: usg60w					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	H-ZYX-USG6-191222/2735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40603		
Product: usg_flex_100w					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	H-ZYX-USG_-191222/2736
Product: usg_flex_200					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	H-ZYX-USG_-191222/2737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**		
Product: usg_flex_500					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	H-ZYX-USG_-191222/2738
Product: usg_flex_50w					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	H-ZYX-USG_-191222/2739
Product: usg_flex_700					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	H-ZYX-USG_-191222/2740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**		
Product: vpn100					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	H-ZYX-VPN1-191222/2741
Product: vpn1000					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	H-ZYX-VPN1-191222/2742
Product: vpn300					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	H-ZYX-VPN3-191222/2743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**		
Product: vpn50					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	H-ZYX-VPN5-191222/2744
Operating System					
Vendor: ami					
Product: megarac_sp-x					
Affected Version(s): 12					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	05-Dec-2022	9.8	MegaRAC Default Credentials Vulnerability **CVE ID : CVE-2022-40242**	N/A	O-AMI-MEGA-201222/2745
N/A	05-Dec-2022	9.8	AMI MegaRAC Redfish Arbitrary Code Execution **CVE ID : CVE-2022-40259**	N/A	O-AMI-MEGA-201222/2746
N/A	05-Dec-2022	7.5	AMI MegaRAC User Enumeration Vulnerability **CVE ID : CVE-2022-2827**	N/A	O-AMI-MEGA-201222/2747
Affected Version(s): 13					
Use of Hard-coded Credentials	05-Dec-2022	9.8	MegaRAC Default Credentials Vulnerability **CVE ID : CVE-2022-40242**	N/A	O-AMI-MEGA-201222/2748
N/A	05-Dec-2022	9.8	AMI MegaRAC Redfish Arbitrary Code Execution **CVE ID : CVE-2022-40259**	N/A	O-AMI-MEGA-201222/2749
N/A	05-Dec-2022	7.5	AMI MegaRAC User Enumeration Vulnerability **CVE ID : CVE-2022-2827**	N/A	O-AMI-MEGA-201222/2750
Vendor: Apple					
Product: macos					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	08-Dec-2022	7.8	In JetBrains IntelliJ IDEA before 2022.2.4 a buffer overflow in the fsnotifier daemon on macOS was possible. **CVE ID : CVE-2022-46824**	https://www.jetbrains.com/privacy-security/issues-fixed/	O-APP-MACO-201222/2751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')					
Unrestricted Upload of File with Dangerous Type	08-Dec-2022	7.8	In JetBrains IntelliJ IDEA before 2022.3 a DYLIB injection on macOS was possible. **CVE ID : CVE-2022-46828**	https://www.jetbrains.com/privacy-security/issues-fixed/	O-APP-MACO-201222/2752
Vendor: Arubanetworks					
Product: arubaos					
Affected Version(s): 10.3.0.0					
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	8.8	Vulnerabilities in ArubaOS running on 7xxx series controllers exist that allows an attacker to execute arbitrary code during the boot sequence. Successful exploitation could allow an attacker to achieve permanent modification of the underlying operating system. **CVE ID : CVE-2022-37904**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2753
Affected Version(s): From (including) 6.5.4.0 Up to (excluding) 6.5.4.22					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Dec-2022	9.8	There is a command injection vulnerability that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of this vulnerability results in the ability to execute	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2022-37897**		
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	8.8	Vulnerabilities in ArubaOS running on 7xxx series controllers exist that allows an attacker to execute arbitrary code during the boot sequence. Successful exploitation could allow an attacker to achieve permanent modification of the underlying operating system. **CVE ID : CVE-2022-37904**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2755
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Dec-2022	8.8	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2022-37912**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2756
Improper Limitation of a Pathname to a Restricted Directory	12-Dec-2022	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of the vulnerability results in the ability to delete	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			arbitrary files on the underlying operating system. **CVE ID : CVE-2022-37906**		
N/A	12-Dec-2022	7.5	A vulnerability exists in the ArubaOS bootloader on 7xxx series controllers which can result in a denial of service (DoS) condition on an impacted system. A successful attacker can cause a system hang which can only be resolved via a power cycle of the impacted controller. **CVE ID : CVE-2022-37907**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2758
N/A	12-Dec-2022	6.5	An authenticated attacker can impact the integrity of the ArubaOS bootloader on 7xxx series controllers. Successful exploitation can compromise the hardware chain of trust on the impacted controller. **CVE ID : CVE-2022-37908**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2759
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Dec-2022	6.5	A buffer overflow vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in a denial of service on the affected system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37910		
Improper Restriction of XML External Entity Reference	12-Dec-2022	5.5	Due to improper restrictions on XML entities multiple vulnerabilities exist in the command line interface of ArubaOS. A successful exploit could allow an authenticated attacker to retrieve files from the local system or cause the application to consume system resources, resulting in a denial of service condition. **CVE ID : CVE-2022-37911**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2761
N/A	12-Dec-2022	5.3	Aruba has identified certain configurations of ArubaOS that can lead to sensitive information disclosure from the configured ESSIDs. The scenarios in which disclosure of potentially sensitive information can occur are complex, and depend on factors beyond the control of attackers. **CVE ID : CVE-2022-37909**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2762
Affected Version(s): From (including) 8.4.0.0 Up to (excluding) 8.6.0.17					
Improper Neutralization of Special Elements used in a Command	12-Dec-2022	9.8	There is a command injection vulnerability that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2022-37897**		
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	8.8	Vulnerabilities in ArubaOS running on 7xxx series controllers exist that allows an attacker to execute arbitrary code during the boot sequence. Successful exploitation could allow an attacker to achieve permanent modification of the underlying operating system. **CVE ID : CVE-2022-37904**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2764
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Dec-2022	8.8	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2022-37912**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Dec-2022	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of the vulnerability results in the ability to delete arbitrary files on the underlying operating system. **CVE ID : CVE-2022-37906**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2766
N/A	12-Dec-2022	7.5	A vulnerability exists in the ArubaOS bootloader on 7xxx series controllers which can result in a denial of service (DoS) condition on an impacted system. A successful attacker can cause a system hang which can only be resolved via a power cycle of the impacted controller. **CVE ID : CVE-2022-37907**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2767
N/A	12-Dec-2022	6.5	An authenticated attacker can impact the integrity of the ArubaOS bootloader on 7xxx series controllers. Successful exploitation can compromise the hardware chain of trust on the impacted controller. **CVE ID : CVE-2022-37908**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2768
Buffer Copy without	12-Dec-2022	6.5	A buffer overflow vulnerability exists in the ArubaOS command line	https://www.arubanetworks.com/assets/	O-ARU-ARUB-201222/2769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface. Successful exploitation of this vulnerability results in a denial of service on the affected system. **CVE ID : CVE-2022-37910**	alert/ARUBA-PSA-2022-016.txt	
Improper Restriction of XML External Entity Reference	12-Dec-2022	5.5	Due to improper restrictions on XML entities multiple vulnerabilities exist in the command line interface of ArubaOS. A successful exploit could allow an authenticated attacker to retrieve files from the local system or cause the application to consume system resources, resulting in a denial of service condition. **CVE ID : CVE-2022-37911**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2770
N/A	12-Dec-2022	5.3	Aruba has identified certain configurations of ArubaOS that can lead to sensitive information disclosure from the configured ESSIDs. The scenarios in which disclosure of potentially sensitive information can occur are complex, and depend on factors beyond the control of attackers. **CVE ID : CVE-2022-37909**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2771
Affected Version(s): From (including) 8.7.0.0 Up to (excluding) 8.7.1.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Dec-2022	9.8	There is a command injection vulnerability that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2022-37897**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2772
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	8.8	Vulnerabilities in ArubaOS running on 7xxx series controllers exist that allows an attacker to execute arbitrary code during the boot sequence. Successful exploitation could allow an attacker to achieve permanent modification of the underlying operating system. **CVE ID : CVE-2022-37904**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2773
Improper Neutralization of Special Elements used in a Command ('Comman	12-Dec-2022	8.8	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities results in the ability to execute arbitrary	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			commands as a privileged user on the underlying operating system. **CVE ID : CVE-2022-37912**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-Dec-2022	8.1	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of the vulnerability results in the ability to delete arbitrary files on the underlying operating system. **CVE ID : CVE-2022-37906**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2775
N/A	12-Dec-2022	7.5	A vulnerability exists in the ArubaOS bootloader on 7xxx series controllers which can result in a denial of service (DoS) condition on an impacted system. A successful attacker can cause a system hang which can only be resolved via a power cycle of the impacted controller. **CVE ID : CVE-2022-37907**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2776
N/A	12-Dec-2022	6.5	An authenticated attacker can impact the integrity of the ArubaOS bootloader on 7xxx series controllers. Successful exploitation can compromise the hardware chain of trust	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the impacted controller. **CVE ID : CVE-2022-37908**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Dec-2022	6.5	A buffer overflow vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in a denial of service on the affected system. **CVE ID : CVE-2022-37910**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2778
Improper Restriction of XML External Entity Reference	12-Dec-2022	5.5	Due to improper restrictions on XML entities multiple vulnerabilities exist in the command line interface of ArubaOS. A successful exploit could allow an authenticated attacker to retrieve files from the local system or cause the application to consume system resources, resulting in a denial of service condition. **CVE ID : CVE-2022-37911**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2779
N/A	12-Dec-2022	5.3	Aruba has identified certain configurations of ArubaOS that can lead to sensitive information disclosure from the configured ESSIDs. The scenarios in which disclosure of potentially sensitive information can occur are complex, and depend on factors	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			beyond the control of attackers. **CVE ID : CVE-2022-37909**		
Affected Version(s): From (including) 8.8.0.0 Up to (excluding) 10.3.0.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Dec-2022	9.8	There is a command injection vulnerability that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2022-37897**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2781
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Dec-2022	8.8	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2022-37912**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2782
Improper Limitation of a	12-Dec-2022	8.1	An authenticated path traversal vulnerability exists in the ArubaOS	https://www.arubanetworks.com/assets/	O-ARU-ARUB-201222/2783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			command line interface. Successful exploitation of the vulnerability results in the ability to delete arbitrary files on the underlying operating system. **CVE ID : CVE-2022-37906**	alert/ARUBA-PSA-2022-016.txt	
N/A	12-Dec-2022	7.5	A vulnerability exists in the ArubaOS bootloader on 7xxx series controllers which can result in a denial of service (DoS) condition on an impacted system. A successful attacker can cause a system hang which can only be resolved via a power cycle of the impacted controller. **CVE ID : CVE-2022-37907**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2784
N/A	12-Dec-2022	6.5	An authenticated attacker can impact the integrity of the ArubaOS bootloader on 7xxx series controllers. Successful exploitation can compromise the hardware chain of trust on the impacted controller. **CVE ID : CVE-2022-37908**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2785
Buffer Copy without Checking Size of Input	12-Dec-2022	6.5	A buffer overflow vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in a	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			denial of service on the affected system. **CVE ID : CVE-2022-37910**		
Improper Restriction of XML External Entity Reference	12-Dec-2022	5.5	Due to improper restrictions on XML entities multiple vulnerabilities exist in the command line interface of ArubaOS. A successful exploit could allow an authenticated attacker to retrieve files from the local system or cause the application to consume system resources, resulting in a denial of service condition. **CVE ID : CVE-2022-37911**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2787
N/A	12-Dec-2022	5.3	Aruba has identified certain configurations of ArubaOS that can lead to sensitive information disclosure from the configured ESSIDs. The scenarios in which disclosure of potentially sensitive information can occur are complex, and depend on factors beyond the control of attackers. **CVE ID : CVE-2022-37909**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt	O-ARU-ARUB-201222/2788
Affected Version(s): From (including) 8.8.0.0 Up to (including) 8.9.03					
Improper Control of Generation of Code	12-Dec-2022	8.8	Vulnerabilities in ArubaOS running on 7xxx series controllers exist that allows an attacker to execute	https://www.arubanetworks.com/assets/alert/ARUBA-	O-ARU-ARUB-201222/2789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			arbitrary code during the boot sequence. Successful exploitation could allow an attacker to achieve permanent modification of the underlying operating system. **CVE ID : CVE-2022-37904**	PSA-2022-016.txt	
Vendor: Asus					
Product: nas-m25_firmware					
Affected Version(s): * Up to (including) 1.0.1.7					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	9.8	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Asus NAS-M25 allows an unauthenticated attacker to inject arbitrary OS commands via unsanitized cookie values.This issue affects NAS-M25: through 1.0.1.7. **CVE ID : CVE-2022-4221**	N/A	O-ASU-NAS--201222/2790
Vendor: BD					
Product: bodyguard_121_twins_firmware					
Affected Version(s): -					
Improper Authentication	05-Dec-2022	5.3	The BD BodyGuard™ infusion pumps specified allow for access through the RS-232 (serial) port interface. If exploited, threat actors with physical access, specialized equipment and knowledge may be able to configure or	https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/bd-bodyguard-pumps-rs-	O-BD-BODY-201222/2791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disable the pump. No electronic protected health information (ePHI), protected health information (PHI) or personally identifiable information (PII) is stored in the pump. **CVE ID : CVE-2022-43557**	232-interface-vulnerability	
Product: bodyguard_323_colorvision_firmware					
Affected Version(s): -					
Improper Authentication	05-Dec-2022	5.3	The BD BodyGuard™ infusion pumps specified allow for access through the RS-232 (serial) port interface. If exploited, threat actors with physical access, specialized equipment and knowledge may be able to configure or disable the pump. No electronic protected health information (ePHI), protected health information (PHI) or personally identifiable information (PII) is stored in the pump. **CVE ID : CVE-2022-43557**	https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/bd-bodyguard-pumps-rs-232-interface-vulnerability	O-BD-BODY-201222/2792
Product: bodyguard_999-603_firmware					
Affected Version(s): -					
Improper Authentication	05-Dec-2022	5.3	The BD BodyGuard™ infusion pumps specified allow for access through the RS-232 (serial) port interface. If exploited, threat actors with physical access,	https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/bd-bodyguard-	O-BD-BODY-201222/2793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specialized equipment and knowledge may be able to configure or disable the pump. No electronic protected health information (ePHI), protected health information (PHI) or personally identifiable information (PII) is stored in the pump. **CVE ID : CVE-2022-43557**	pumps-rs-232-interface-vulnerability	
Product: bodyguard_duo_999-903_firmware					
Affected Version(s): -					
Improper Authentication	05-Dec-2022	5.3	The BD BodyGuard™ infusion pumps specified allow for access through the RS-232 (serial) port interface. If exploited, threat actors with physical access, specialized equipment and knowledge may be able to configure or disable the pump. No electronic protected health information (ePHI), protected health information (PHI) or personally identifiable information (PII) is stored in the pump. **CVE ID : CVE-2022-43557**	https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/bd-bodyguard-pumps-rs-232-interface-vulnerability	O-BD-BODY-201222/2794
Product: bodyguard_epidural_999-683_firmware					
Affected Version(s): -					
Improper Authentication	05-Dec-2022	5.3	The BD BodyGuard™ infusion pumps specified allow for access through the RS-232 (serial) port	https://www.bd.com/en-us/about-bd/cybersecu	O-BD-BODY-201222/2795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface. If exploited, threat actors with physical access, specialized equipment and knowledge may be able to configure or disable the pump. No electronic protected health information (ePHI), protected health information (PHI) or personally identifiable information (PII) is stored in the pump. **CVE ID : CVE-2022-43557**	rity/bulletin/bd-bodyguard-pumps-rs-232-interface-vulnerability	
Product: bodyguard_pain_manager_999-803_firmware					
Affected Version(s): -					
Improper Authentication	05-Dec-2022	5.3	The BD BodyGuard™ infusion pumps specified allow for access through the RS-232 (serial) port interface. If exploited, threat actors with physical access, specialized equipment and knowledge may be able to configure or disable the pump. No electronic protected health information (ePHI), protected health information (PHI) or personally identifiable information (PII) is stored in the pump. **CVE ID : CVE-2022-43557**	https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/bd-bodyguard-pumps-rs-232-interface-vulnerability	O-BD-BODY-201222/2796
Product: bodyguard_t_999-103_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	05-Dec-2022	5.3	The BD BodyGuard™ infusion pumps specified allow for access through the RS-232 (serial) port interface. If exploited, threat actors with physical access, specialized equipment and knowledge may be able to configure or disable the pump. No electronic protected health information (ePHI), protected health information (PHI) or personally identifiable information (PII) is stored in the pump. **CVE ID : CVE-2022-43557**	https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/bd-bodyguard-pumps-rs-232-interface-vulnerability	O-BD-BODY-201222/2797
Vendor: Brocade					
Product: fabric_operating_system					
Affected Version(s): 7.4.2j					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-2022	9.8	A vulnerability in Brocade Fabric OS software v9.1.1, v9.0.1e, v8.2.3c, v7.4.2j, and earlier versions could allow a remote unauthenticated attacker to execute on a Brocade Fabric OS switch commands capable of modifying zoning, disabling the switch, disabling ports, and modifying the switch IP address. **CVE ID : CVE-2022-33186**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2121	O-BRO-FABR-201222/2798
Affected Version(s): 8.2.3c					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-2022	9.8	A vulnerability in Brocade Fabric OS software v9.1.1, v9.0.1e, v8.2.3c, v7.4.2j, and earlier versions could allow a remote unauthenticated attacker to execute on a Brocade Fabric OS switch commands capable of modifying zoning, disabling the switch, disabling ports, and modifying the switch IP address. **CVE ID : CVE-2022-33186**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2121	O-BRO-FABR-201222/2799
Affected Version(s): 9.0.1e					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Dec-2022	9.8	A vulnerability in Brocade Fabric OS software v9.1.1, v9.0.1e, v8.2.3c, v7.4.2j, and earlier versions could allow a remote unauthenticated attacker to execute on a Brocade Fabric OS switch commands capable of modifying zoning, disabling the switch, disabling ports, and modifying the switch IP address. **CVE ID : CVE-2022-33186**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2022-2121	O-BRO-FABR-201222/2800
Affected Version(s): 9.1.1					
Improper Neutralization of Special Elements used in an	08-Dec-2022	9.8	A vulnerability in Brocade Fabric OS software v9.1.1, v9.0.1e, v8.2.3c, v7.4.2j, and earlier versions could allow a remote	https://www.broadcom.com/support/fibre-channel-networking/security-	O-BRO-FABR-201222/2801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			unauthenticated attacker to execute on a Brocade Fabric OS switch commands capable of modifying zoning, disabling the switch, disabling ports, and modifying the switch IP address. **CVE ID : CVE-2022-33186**	advisories/brocade-security-advisory-2022-2121	
Vendor: Buffalo					
Product: bhr-4grv_firmware					
Affected Version(s): * Up to (including) 2.00					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-BHR--201222/2802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-BHR--201222/2803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: dwr-hp-g300nh_firmware					
Affected Version(s): * Up to (including) 1.84					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-DWR--201222/2804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-DWR--201222/2805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: dwr-pg_firmware					
Affected Version(s): * Up to (including) 1.83					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-DWR--201222/2806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-DWR--201222/2807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: fs-600dhp_firmware					
Affected Version(s): * Up to (including) 3.40					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-FS-6-201222/2808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver.	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-FS-6-201222/2809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: fs-g300n_firmware					
Affected Version(s): * Up to (including) 3.14					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-FS-G-201222/2810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-FS-G-201222/2811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: fs-hp-g300n_firmware					
Affected Version(s): * Up to (including) 3.33					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-FS-H-201222/2812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-FS-H-201222/2813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39044		
Product: fs-r600dhp_firmware					
Affected Version(s): * Up to (including) 3.40					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-FS-R-201222/2814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-FS-R-201222/2815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: hw-450hp-zwe_firmware					
Affected Version(s): * Up to (including) 2.00					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-HW-4-201222/2816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-HW-4-201222/2817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Use of Hard-coded Credentials	07-Dec-2022	6.5	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, and WZR-D1100H firmware Ver. 2.00 and earlier. **CVE ID : CVE-2022-34840**	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-HW-4-201222/2818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wcr-300_firmware					
Affected Version(s): * Up to (including) 1.87					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WCR--201222/2819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WCR--201222/2820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wem-1266wp_firmware					
Affected Version(s): * Up to (including) 2.85					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WEM--201222/2821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wem-1266_firmware					
Affected Version(s): * Up to (including) 2.85					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WEM--201222/2822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wer-a54g54_firmware					
Affected Version(s): * Up to (including) 1.43					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WER--201222/2823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40966		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WER--201222/2824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wer-ag54_firmware					
Affected Version(s): * Up to (including) 1.43					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-	https://www.buffalo.jp/news/detail/20	O-BUF-WER--201222/2825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H	221003-01.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WER--201222/2826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wer-am54g54_firmware					
Affected Version(s): * Up to (including) 1.43					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WER--201222/2827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WER--201222/2828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wer-amg54_firmware					
Affected Version(s): * Up to (including) 1.43					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WER--201222/2829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-	https://www.buffalo.jp/news/detail/20	O-BUF-WER--201222/2830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and	221003-01.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-300hp_firmware					
Affected Version(s): * Up to (including) 2.00					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-300_firmware					
Affected Version(s): * Up to (including) 2.00					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-am54g54_firmware					
Affected Version(s): * Up to (including) 1.43					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-amg54_firmware					
Affected Version(s): * Up to (including) 1.43					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-ampg_firmware					
Affected Version(s): * Up to (including) 1.52					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver.	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-g300n_firmware					
Affected Version(s): * Up to (including) 1.65					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-g301n_firmware					
Affected Version(s): * Up to (including) 1.87					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39044		
Product: whr-g54s-ni_firmware					
Affected Version(s): * Up to (including) 1.24					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-g54s_firmware					
Affected Version(s): * Up to (including) 1.43					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-g_firmware					
Affected Version(s): * Up to (including) 1.49					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-hp-ampg_firmware					
Affected Version(s): * Up to (including) 1.43					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Affected Version(s): * Up to (including) 1.49					
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-hp-g300n_firmware					
Affected Version(s): * Up to (including) 2.00					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-hp-g54_firmware					
Affected Version(s): * Up to (including) 1.43					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver.	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-hp-gn_firmware					
Affected Version(s): * Up to (including) 1.87					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: whr-hp-g_firmware					
Affected Version(s): * Up to (including) 1.49					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WHR--201222/2860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39044		
Product: wlae-ag300n_firmware					
Affected Version(s): * Up to (including) 1.86					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WLAE-201222/2861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WLAE-201222/2862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wli-h4-d600_firmware					
Affected Version(s): * Up to (including) 1.88					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WLI--201222/2863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WLI--201222/2864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wli-tx4-ag300n_firmware					
Affected Version(s): * Up to (including) 1.53					
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WLI--201222/2865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wpl-05g300_firmware					
Affected Version(s): * Up to (including) 1.88					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WPL--201222/2866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple	https://www.buffalo.jp/ne	O-BUF-WPL--201222/2867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and	ws/detail/20221003-01.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wrm-d2133hp_firmware					
Affected Version(s): * Up to (including) 2.85					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WRM--201222/2868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wrm-d2133hs_firmware					
Affected Version(s): * Up to (including) 2.96					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WRM--201222/2869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: ws024bf-nw_firmware					
Affected Version(s): * Up to (including) 1.60					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WS02-201222/2870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WS02-201222/2871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: ws024bf_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.60					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WS02-201222/2872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WS02-201222/2873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wtr-m2133hp_firmware					
Affected Version(s): * Up to (including) 2.85					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WTR--201222/2874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wtr-m2133hs_firmware					
Affected Version(s): * Up to (including) 2.96					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WTR--201222/2875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wxr-1750dhp2_firmware					
Affected Version(s): * Up to (including) 2.60					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WXR--201222/2876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wxr-1750dhp_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.60					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WXR--201222/2877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wxr-1900dhp2_firmware					
Affected Version(s): * Up to (including) 2.59					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WXR--201222/2878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wxr-1900dhp3_firmware					
Affected Version(s): * Up to (including) 2.63					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WXR--201222/2879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wxr-1900dhp_firmware					
Affected Version(s): * Up to (including) 2.50					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WXR--201222/2880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wxr-5950ax12_firmware					
Affected Version(s): * Up to (including) 3.40					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WXR--201222/2881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wxr-6000ax12b_firmware					
Affected Version(s): * Up to (including) 3.40					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WXR--201222/2882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wxr-6000ax12s_firmware					
Affected Version(s): * Up to (including) 3.40					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WXR--201222/2883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr-1166dhp2_firmware					
Affected Version(s): * Up to (including) 2.18					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr-1166dhp_firmware					
Affected Version(s): * Up to (including) 2.18					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr-1750dhp2_firmware					
Affected Version(s): * Up to (including) 2.31					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr-1750dhp_firmware					
Affected Version(s): * Up to (including) 2.30					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr-300hp_firmware					
Affected Version(s): * Up to (including) 2.00					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Use of Hard-coded Credentials	07-Dec-2022	6.5	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-D1100H firmware Ver. 2.00 and earlier. **CVE ID : CVE-2022-34840**		
Product: wzr-450hp-cwt_firmware					
Affected Version(s): * Up to (including) 2.00					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-	https://www.buffalo.jp/news/detail/20	O-BUF-WZR--201222/2892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and	221003-01.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Use of Hard-coded Credentials	07-Dec-2022	6.5	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, and WZR-D1100H firmware Ver. 2.00 and earlier. **CVE ID : CVE-2022-34840**		
Product: wzr-450hp-ub_firmware					
Affected Version(s): * Up to (including) 2.00					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39044		
Use of Hard-coded Credentials	07-Dec-2022	6.5	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, and WZR-D1100H firmware Ver. 2.00 and earlier. **CVE ID : CVE-2022-34840**	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2896
Product: wzr-450hp_firmware					
Affected Version(s): * Up to (including) 2.00					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device.	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Use of Hard-coded Credentials	07-Dec-2022	6.5	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver.	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.15 and earlier, and WZR-D1100H firmware Ver. 2.00 and earlier. **CVE ID : CVE-2022-34840**		
Product: wzr-600dhp2_firmware					
Affected Version(s): * Up to (including) 1.15					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices	https://www.buffalo.jp/news/detail/20	O-BUF-WZR--201222/2901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE	221003-01.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Use of Hard-coded Credentials	07-Dec-2022	6.5	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, and WZR-D1100H firmware Ver. 2.00 and earlier. **CVE ID : CVE-2022-34840**		
Product: wzr-600dhp3_firmware					
Affected Version(s): * Up to (including) 2.19					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr-600dhp_firmware					
Affected Version(s): * Up to (including) 2.00					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40966		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Use of Hard-coded Credentials	07-Dec-2022	6.5	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, and WZR-D1100H firmware Ver. 2.00 and earlier. **CVE ID : CVE-2022-34840**		
Product: wzr-900dhp2_firmware					
Affected Version(s): * Up to (including) 2.19					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr-900dhp_firmware					
Affected Version(s): * Up to (including) 1.15					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	07-Dec-2022	6.5	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, and WZR-D1100H firmware Ver. 2.00 and earlier. **CVE ID : CVE-2022-34840**	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2910
Product: wzr-agl300nh_firmware					
Affected Version(s): * Up to (including) 1.55					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr-ampg144nh_firmware					
Affected Version(s): * Up to (including) 1.49					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr-ampg300nh_firmware					
Affected Version(s): * Up to (including) 1.51					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr-d1100h_firmware					
Affected Version(s): * Up to (including) 2.00					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Use of Hard-coded Credentials	07-Dec-2022	6.5	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, and WZR-D1100H firmware Ver. 2.00 and earlier. **CVE ID : CVE-2022-34840**	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2919
Product: wzr-g144nh_firmware					
Affected Version(s): * Up to (including) 1.48					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr-g144n_firmware					
Affected Version(s): * Up to (including) 1.48					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr-hp-ag300h_firmware					
Affected Version(s): * Up to (including) 1.76					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver.	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr-hp-g300nh_firmware					
Affected Version(s): * Up to (including) 1.84					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr-hp-g301nh_firmware					
Affected Version(s): * Up to (including) 1.84					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39044		
Product: wzr-hp-g302h_firmware					
Affected Version(s): * Up to (including) 1.86					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr-hp-g450h_firmware					
Affected Version(s): * Up to (including) 1.90					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr-s1750dhp_firmware					
Affected Version(s): * Up to (including) 2.32					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr-s600dhp_firmware					
Affected Version(s): * Up to (including) 2.19					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr-s900dhp_firmware					
Affected Version(s): * Up to (including) 2.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR--201222/2936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
Product: wzr2-g108_firmware					
Affected Version(s): * Up to (including) 1.33					
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR2-201222/2937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Product: wzr2-g300n_firmware					
Affected Version(s): * Up to (including) 1.55					
Improper Authentication	07-Dec-2022	8.8	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR2-201222/2938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier. **CVE ID : CVE-2022-40966**		
N/A	07-Dec-2022	6.8	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and	https://www.buffalo.jp/news/detail/20221003-01.html	O-BUF-WZR2-201222/2939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier. **CVE ID : CVE-2022-39044**		
Vendor: Cisco					
Product: ata_190_firmware					
Affected Version(s): -					
Improper Input Validation	12-Dec-2022	8.8	Multiple vulnerabilities in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause Cisco Discovery Protocol memory corruption on an affected device. These vulnerabilities are due to missing length validation checks when processing Cisco Discovery Protocol messages. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read of the valid Cisco Discovery Protocol packet data, which could allow the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause corruption in the internal Cisco Discovery Protocol database of the affected device. **CVE ID : CVE-2022-20689**		
Improper Input Validation	12-Dec-2022	8.8	Multiple vulnerabilities in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause Cisco Discovery Protocol memory corruption on an affected device. These vulnerabilities are due to missing length validation checks when processing Cisco Discovery Protocol messages. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read of the valid Cisco Discovery Protocol packet data, which could allow the attacker to cause corruption in the internal Cisco Discovery Protocol database of the affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20690		
Uncontrolled Resource Consumption	12-Dec-2022	6.5	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Adaptive Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause a DoS condition of an affected device. This vulnerability is due to missing length validation of certain Cisco Discovery Protocol packet header fields. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol packets to an affected device. A successful exploit could allow the attacker to cause the device to exhaust available memory and cause the service to restart. Cisco has released firmware updates that address this vulnerability. **CVE ID : CVE-2022-20691**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2942
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	5.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code on an affected device and cause the LLDP service to restart. These vulnerabilities are due to missing length validation of certain LLDP packet header fields. An attacker could exploit these vulnerabilities by sending a malicious LLDP packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause LLDP to restart unexpectedly, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20686**		
Improper Input Validation	12-Dec-2022	5.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause the LLDP service to restart. These vulnerabilities are due to missing length validation of certain LLDP packet header fields. An attacker could exploit these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities by sending a malicious LLDP packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause LLDP to restart unexpectedly, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20687**		
Improper Input Validation	12-Dec-2022	5.3	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause Cisco Discovery Protocol service to restart. This vulnerability is due to missing length validation of certain Cisco Discovery Protocol packet header fields. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause Cisco Discovery Protocol to restart unexpectedly,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a DoS condition. **CVE ID : CVE-2022-20688**		
Product: ata_191_firmware					
Affected Version(s): * Up to (excluding) 11.2.2					
Improper Input Validation	12-Dec-2022	8.8	Multiple vulnerabilities in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause Cisco Discovery Protocol memory corruption on an affected device. These vulnerabilities are due to missing length validation checks when processing Cisco Discovery Protocol messages. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read of the valid Cisco Discovery Protocol packet data, which could allow the attacker to cause corruption in the internal Cisco Discovery Protocol database of the affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20689		
Improper Input Validation	12-Dec-2022	8.8	Multiple vulnerabilities in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause Cisco Discovery Protocol memory corruption on an affected device. These vulnerabilities are due to missing length validation checks when processing Cisco Discovery Protocol messages. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read of the valid Cisco Discovery Protocol packet data, which could allow the attacker to cause corruption in the internal Cisco Discovery Protocol database of the affected device. **CVE ID : CVE-2022-20690**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2947
Uncontrolled Resource	12-Dec-2022	6.5	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Adaptive	https://tools.cisco.com/security/center/content/Cisco	O-CIS-ATA_-201222/2948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause a DoS condition of an affected device. This vulnerability is due to missing length validation of certain Cisco Discovery Protocol packet header fields. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol packets to an affected device. A successful exploit could allow the attacker to cause the device to exhaust available memory and cause the service to restart. Cisco has released firmware updates that address this vulnerability. **CVE ID : CVE-2022-20691**	SecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	5.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause the LLDP service to restart. These vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing length validation of certain LLDP packet header fields. An attacker could exploit these vulnerabilities by sending a malicious LLDP packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause LLDP to restart unexpectedly, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20686**		
Improper Input Validation	12-Dec-2022	5.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause the LLDP service to restart. These vulnerabilities are due to missing length validation of certain LLDP packet header fields. An attacker could exploit these vulnerabilities by sending a malicious LLDP packet to an affected device. A successful exploit could allow the attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute code on the affected device and cause LLDP to restart unexpectedly, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20687**		
Improper Input Validation	12-Dec-2022	5.3	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause Cisco Discovery Protocol service to restart. This vulnerability is due to missing length validation of certain Cisco Discovery Protocol packet header fields. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause Cisco Discovery Protocol to restart unexpectedly, resulting in a DoS condition. **CVE ID : CVE-2022-20688**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2951
Affected Version(s): * Up to (excluding) 12.0.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Dec-2022	8.8	Multiple vulnerabilities in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause Cisco Discovery Protocol memory corruption on an affected device. These vulnerabilities are due to missing length validation checks when processing Cisco Discovery Protocol messages. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read of the valid Cisco Discovery Protocol packet data, which could allow the attacker to cause corruption in the internal Cisco Discovery Protocol database of the affected device. **CVE ID : CVE-2022-20689**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2952
Improper Input Validation	12-Dec-2022	8.8	Multiple vulnerabilities in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-ATA_-201222/2953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated, adjacent attacker to cause Cisco Discovery Protocol memory corruption on an affected device. These vulnerabilities are due to missing length validation checks when processing Cisco Discovery Protocol messages. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read of the valid Cisco Discovery Protocol packet data, which could allow the attacker to cause corruption in the internal Cisco Discovery Protocol database of the affected device. **CVE ID : CVE-2022-20690**	ata19x-multivuln-GEZYVvs	
Uncontrolled Resource Consumption	12-Dec-2022	6.5	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Adaptive Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause a DoS condition of an affected device. This vulnerability is due to missing length validation	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of certain Cisco Discovery Protocol packet header fields. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol packets to an affected device. A successful exploit could allow the attacker to cause the device to exhaust available memory and cause the service to restart. Cisco has released firmware updates that address this vulnerability. **CVE ID : CVE-2022-20691**		
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	5.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause the LLDP service to restart. These vulnerabilities are due to missing length validation of certain LLDP packet header fields. An attacker could exploit these vulnerabilities by sending a malicious LLDP packet to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute code on the affected device and cause LLDP to restart unexpectedly, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20686**		
Improper Input Validation	12-Dec-2022	5.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause the LLDP service to restart. These vulnerabilities are due to missing length validation of certain LLDP packet header fields. An attacker could exploit these vulnerabilities by sending a malicious LLDP packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause LLDP to restart unexpectedly, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20687**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-Dec-2022	5.3	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause Cisco Discovery Protocol service to restart. This vulnerability is due to missing length validation of certain Cisco Discovery Protocol packet header fields. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause Cisco Discovery Protocol to restart unexpectedly, resulting in a DoS condition. **CVE ID : CVE-2022-20688**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2957
Affected Version(s): 12.0.1					
Improper Input Validation	12-Dec-2022	8.8	Multiple vulnerabilities in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause Cisco Discovery Protocol memory corruption on an affected device. These vulnerabilities are due to missing length validation checks when processing Cisco Discovery Protocol messages. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read of the valid Cisco Discovery Protocol packet data, which could allow the attacker to cause corruption in the internal Cisco Discovery Protocol database of the affected device. **CVE ID : CVE-2022-20689**		
Improper Input Validation	12-Dec-2022	8.8	Multiple vulnerabilities in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause Cisco Discovery Protocol memory corruption on an affected device. These vulnerabilities are due to missing length validation	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checks when processing Cisco Discovery Protocol messages. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read of the valid Cisco Discovery Protocol packet data, which could allow the attacker to cause corruption in the internal Cisco Discovery Protocol database of the affected device. **CVE ID : CVE-2022-20690**		
Uncontrolled Resource Consumption	12-Dec-2022	6.5	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Adaptive Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause a DoS condition of an affected device. This vulnerability is due to missing length validation of certain Cisco Discovery Protocol packet header fields. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol packets to an affected device. A successful	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause the device to exhaust available memory and cause the service to restart. Cisco has released firmware updates that address this vulnerability. **CVE ID : CVE-2022-20691**		
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	5.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause the LLDP service to restart. These vulnerabilities are due to missing length validation of certain LLDP packet header fields. An attacker could exploit these vulnerabilities by sending a malicious LLDP packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause LLDP to restart unexpectedly, resulting in a denial of service (DoS) condition.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20686		
Improper Input Validation	12-Dec-2022	5.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause the LLDP service to restart. These vulnerabilities are due to missing length validation of certain LLDP packet header fields. An attacker could exploit these vulnerabilities by sending a malicious LLDP packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause LLDP to restart unexpectedly, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20687**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2962
Improper Input Validation	12-Dec-2022	5.3	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-	O-CIS-ATA_-201222/2963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code on an affected device and cause Cisco Discovery Protocol service to restart. This vulnerability is due to missing length validation of certain Cisco Discovery Protocol packet header fields. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause Cisco Discovery Protocol to restart unexpectedly, resulting in a DoS condition. **CVE ID : CVE-2022-20688**	multivuln-GEZYVvs	
Product: ata_192_firmware					
Affected Version(s): * Up to (excluding) 11.2.2					
Improper Input Validation	12-Dec-2022	8.8	Multiple vulnerabilities in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause Cisco Discovery Protocol memory corruption on an affected device. These vulnerabilities are due to missing length validation checks when processing	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco Discovery Protocol messages. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read of the valid Cisco Discovery Protocol packet data, which could allow the attacker to cause corruption in the internal Cisco Discovery Protocol database of the affected device. **CVE ID : CVE-2022-20689**		
Improper Input Validation	12-Dec-2022	8.8	Multiple vulnerabilities in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause Cisco Discovery Protocol memory corruption on an affected device. These vulnerabilities are due to missing length validation checks when processing Cisco Discovery Protocol messages. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packet to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read of the valid Cisco Discovery Protocol packet data, which could allow the attacker to cause corruption in the internal Cisco Discovery Protocol database of the affected device. **CVE ID : CVE-2022-20690**		
Uncontrolled Resource Consumption	12-Dec-2022	6.5	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Adaptive Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause a DoS condition of an affected device. This vulnerability is due to missing length validation of certain Cisco Discovery Protocol packet header fields. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol packets to an affected device. A successful exploit could allow the attacker to cause the device to exhaust available memory and cause the service to restart. Cisco has released firmware	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates that address this vulnerability. **CVE ID : CVE-2022-20691**		
Improper Control of Generation of Code ('Code Injection')	12-Dec-2022	5.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause the LLDP service to restart. These vulnerabilities are due to missing length validation of certain LLDP packet header fields. An attacker could exploit these vulnerabilities by sending a malicious LLDP packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause LLDP to restart unexpectedly, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20686**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2967
Improper Input Validation	12-Dec-2022	5.3	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) functionality of Cisco ATA 190 Series Analog Telephone	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-ATA_-201222/2968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause the LLDP service to restart. These vulnerabilities are due to missing length validation of certain LLDP packet header fields. An attacker could exploit these vulnerabilities by sending a malicious LLDP packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause LLDP to restart unexpectedly, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2022-20687**	ata19x-multivuln-GEZYVvs	
Improper Input Validation	12-Dec-2022	5.3	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause Cisco Discovery Protocol service to restart. This vulnerability is due to missing length validation of certain Cisco Discovery Protocol	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs	O-CIS-ATA_-201222/2969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packet header fields. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause Cisco Discovery Protocol to restart unexpectedly, resulting in a DoS condition. **CVE ID : CVE-2022-20688**		
Product: ip_phone_7811_firmware					
Affected Version(s): 10.1\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2971
Affected Version(s): 10.1\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/2972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.2\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.2\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 10.2\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2975
Affected Version(s): 10.3\\(1.11\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2978
Affected Version(s): 10.3\\(1\\)sr1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2979
Affected Version(s): 10.3\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr4					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2982
Affected Version(s): 10.3\\(1\\)sr4b					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/2983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.3\\(1\\)sr5					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr6					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 10.3\\(1\\)sr7					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2986
Affected Version(s): 10.3\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.4\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.4\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2989
Affected Version(s): 11-0-1msr1-1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2990
Affected Version(s): 11.0\\(0.7\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2993
Affected Version(s): 11.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/2994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 11.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2997
Affected Version(s): 12.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/2999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3000
Affected Version(s): 12.1\\(1\\)sr1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3001
Affected Version(s): 12.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3004
Affected Version(s): 12.5\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.6\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.6\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3008
Affected Version(s): 12.7\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.8\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.8\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3011
Affected Version(s): 12.8\\(1\\)sr2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3012
Affected Version(s): 14.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3015
Affected Version(s): 14.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 14.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 9.3\\(3\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3019
Affected Version(s): 9.3\\(4\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3022
Affected Version(s): 9.3\\(4\\)sr3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3023
Product: ip_phone_7821_firmware					
Affected Version(s): 10.1\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.1\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3026
Affected Version(s): 10.2\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of	https://tools.cisco.com/security/center/	O-CIS-IP_P-201222/3027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	content/Cisco SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.2\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.2\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1.11\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3030
Affected Version(s): 10.3\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-IP_P-201222/3031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.3\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 10.3\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3034
Affected Version(s): 10.3\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr4					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr4b					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3037
Affected Version(s): 10.3\\(1\\)sr5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3038
Affected Version(s): 10.3\\(1\\)sr6					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr7					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3041
Affected Version(s): 10.4\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.4\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11-0-1msr1-1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 11.0\\(0.7\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3045
Affected Version(s): 11.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3048
Affected Version(s): 11.7\\(1\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3049
Affected Version(s): 12.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3052
Affected Version(s): 12.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3056
Affected Version(s): 12.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3059
Affected Version(s): 12.6\\(1\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3060
Affected Version(s): 12.6\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.7\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3063
Affected Version(s): 12.8\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.8\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.8\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 14.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3067
Affected Version(s): 14.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3070
Affected Version(s): 14.1\\(1\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3071
Affected Version(s): 14.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(3\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3074
Affected Version(s): 9.3\\(4\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 9.3\\(4\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Product: ip_phone_7832_firmware					
Affected Version(s): 10.1\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3078
Affected Version(s): 10.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-IP_P-201222/3079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.1\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.2\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 10.2\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3082
Affected Version(s): 10.2\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1.11\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3085
Affected Version(s): 10.3\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of	https://tools.cisco.com/security/center/	O-CIS-IP_P-201222/3086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	content/Cisco SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.3\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3089
Affected Version(s): 10.3\\(1\\)sr4					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-IP_P-201222/3090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.3\\(1\\)sr4b					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr5					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 10.3\\(1\\)sr6					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3093
Affected Version(s): 10.3\\(1\\)sr7					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.4\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3096
Affected Version(s): 10.4\\(1\\)sr2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3097
Affected Version(s): 11-0-1msr1-1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.0\\(0.7\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3100
Affected Version(s): 11.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 11.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3104
Affected Version(s): 12.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3107
Affected Version(s): 12.1\\(1\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3108
Affected Version(s): 12.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3111
Affected Version(s): 12.5\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.5\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.6\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.6\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3115
Affected Version(s): 12.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.7\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.8\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3118
Affected Version(s): 12.8\\(1\\)sr1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3119
Affected Version(s): 12.8\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3122
Affected Version(s): 14.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 14.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 14.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3126
Affected Version(s): 9.3\\(3\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3129
Affected Version(s): 9.3\\(4\\)sr2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3130
Affected Version(s): 9.3\\(4\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Product: ip_phone_7841_firmware					
Affected Version(s): 10.1\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3133
Affected Version(s): 10.1\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of	https://tools.cisco.com/security/center/	O-CIS-IP_P-201222/3134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	content/Cisco SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.2\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.2\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.2\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3137
Affected Version(s): 10.3\\(1.11\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-IP_P-201222/3138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.3\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 10.3\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3141
Affected Version(s): 10.3\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr4					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3144
Affected Version(s): 10.3\\(1\\)sr4b					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3145
Affected Version(s): 10.3\\(1\\)sr5					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr6					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr7					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3148
Affected Version(s): 10.3\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.4\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.4\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 11-0-1msr1-1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3152
Affected Version(s): 11.0\\(0.7\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3155
Affected Version(s): 11.5\\(1\\)sr1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3156
Affected Version(s): 11.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3159
Affected Version(s): 12.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3163
Affected Version(s): 12.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3166
Affected Version(s): 12.5\\(1\\)sr3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3167
Affected Version(s): 12.6\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.6\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3170
Affected Version(s): 12.7\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.8\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.8\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.8\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3174
Affected Version(s): 14.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3177
Affected Version(s): 14.0\\(1\\)sr3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3178
Affected Version(s): 14.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(3\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3181
Affected Version(s): 9.3\\(4\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 9.3\\(4\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 9.3\\(4\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3185
Product: ip_phone_7861_firmware					
Affected Version(s): 10.1\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-IP_P-201222/3186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.1\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 10.2\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3189
Affected Version(s): 10.2\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.2\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1.11\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3192
Affected Version(s): 10.3\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of	https://tools.cisco.com/security/center/	O-CIS-IP_P-201222/3193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	content/Cisco SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.3\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3196
Affected Version(s): 10.3\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-IP_P-201222/3197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.3\\(1\\)sr4					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr4b					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 10.3\\(1\\)sr5					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3200
Affected Version(s): 10.3\\(1\\)sr6					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr7					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3203
Affected Version(s): 10.4\\(1\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3204
Affected Version(s): 10.4\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11-0-1msr1-1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.0\\(0.7\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3207
Affected Version(s): 11.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 11.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 11.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3211
Affected Version(s): 12.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3214
Affected Version(s): 12.0\\(1\\)sr3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3215
Affected Version(s): 12.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3218
Affected Version(s): 12.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.5\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.6\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3222
Affected Version(s): 12.6\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.7\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3225
Affected Version(s): 12.8\\(1\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3226
Affected Version(s): 12.8\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.8\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3229
Affected Version(s): 14.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 14.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 14.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3233
Affected Version(s): 14.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(3\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3236
Affected Version(s): 9.3\\(4\\)sr1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3237
Affected Version(s): 9.3\\(4\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Product: ip_phone_8811_firmware					
Affected Version(s): 10.1\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3240
Affected Version(s): 10.1\\(1\\)sr1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3241
Affected Version(s): 10.1\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.2\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.2\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3244
Affected Version(s): 10.2\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.3\\(1.11\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 10.3\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3248
Affected Version(s): 10.3\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3251
Affected Version(s): 10.3\\(1\\)sr4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3252
Affected Version(s): 10.3\\(1\\)sr4b					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr5					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr6					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3255
Affected Version(s): 10.3\\(1\\)sr7					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.3\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.4\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 10.4\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3259
Affected Version(s): 11-0-1msr1-1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.0\\(0.7\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3262
Affected Version(s): 11.5\\(1\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3263
Affected Version(s): 11.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3266
Affected Version(s): 12.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3270
Affected Version(s): 12.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3273
Affected Version(s): 12.5\\(1\\)sr2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3274
Affected Version(s): 12.5\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.6\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.6\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3277
Affected Version(s): 12.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.7\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.8\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.8\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3281
Affected Version(s): 12.8\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3284
Affected Version(s): 14.0\\(1\\)sr2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3285
Affected Version(s): 14.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3288
Affected Version(s): 9.3\\(3\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 9.3\\(4\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 9.3\\(4\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3292
Affected Version(s): 9.3\\(4\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Product: ip_phone_8831_firmware					
Affected Version(s): 10.1\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 10.1\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3296
Affected Version(s): 10.2\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.2\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.2\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3299
Affected Version(s): 10.3\\(1.11\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of	https://tools.cisco.com/security/center/	O-CIS-IP_P-201222/3300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	content/Cisco SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.3\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3303
Affected Version(s): 10.3\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-IP_P-201222/3304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.3\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr4					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 10.3\\(1\\)sr4b					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3307
Affected Version(s): 10.3\\(1\\)sr5					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr6					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr7					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3310
Affected Version(s): 10.3\\(2\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3311
Affected Version(s): 10.4\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.4\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11-0-1msr1-1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3314
Affected Version(s): 11.0\\(0.7\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 11.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 11.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3318
Affected Version(s): 11.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3321
Affected Version(s): 12.0\\(1\\)sr2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3322
Affected Version(s): 12.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3325
Affected Version(s): 12.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.5\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3329
Affected Version(s): 12.6\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.6\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3332
Affected Version(s): 12.7\\(1\\)sr1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3333
Affected Version(s): 12.8\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.8\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.8\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3336
Affected Version(s): 14.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 14.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 14.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3340
Affected Version(s): 14.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(3\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3343
Affected Version(s): 9.3\\(4\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3344
Affected Version(s): 9.3\\(4\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3347
Product: ip_phone_8832_firmware					
Affected Version(s): 10.1\\(1.9\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3348
Affected Version(s): 10.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.1\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.2\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3351
Affected Version(s): 10.2\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.2\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1.11\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 10.3\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3355
Affected Version(s): 10.3\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3358
Affected Version(s): 10.3\\(1\\)sr3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3359
Affected Version(s): 10.3\\(1\\)sr4					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr4b					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr5					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3362
Affected Version(s): 10.3\\(1\\)sr6					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.3\\(1\\)sr7					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 10.4\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3366
Affected Version(s): 10.4\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11-0-1msr1-1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.0\\(0.7\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3369
Affected Version(s): 11.0\\(1\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3370
Affected Version(s): 11.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3373
Affected Version(s): 12.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3377
Affected Version(s): 12.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3380
Affected Version(s): 12.5\\(1\\)sr1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3381
Affected Version(s): 12.5\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.6\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3384
Affected Version(s): 12.6\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.7\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.8\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3388
Affected Version(s): 12.8\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.8\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3391
Affected Version(s): 14.0\\(1\\)sr1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3392
Affected Version(s): 14.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3395
Affected Version(s): 14.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 9.3\\(3\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 9.3\\(4\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3399
Affected Version(s): 9.3\\(4\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Product: ip_phone_8841_firmware					
Affected Version(s): 10.1\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 10.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3403
Affected Version(s): 10.1\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.2\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.2\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3406
Affected Version(s): 10.2\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of	https://tools.cisco.com/security/center/	O-CIS-IP_P-201222/3407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	content/Cisco SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.3\\(1.11\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3410
Affected Version(s): 10.3\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-IP_P-201222/3411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.3\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 10.3\\(1\\)sr4					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3414
Affected Version(s): 10.3\\(1\\)sr4b					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr5					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr6					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3417
Affected Version(s): 10.3\\(1\\)sr7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3418
Affected Version(s): 10.3\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.4\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.4\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3421
Affected Version(s): 11-0-1msr1-1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 11.0\\(0.7\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 11.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3425
Affected Version(s): 11.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3428
Affected Version(s): 12.0\\(1\\)sr1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3429
Affected Version(s): 12.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3432
Affected Version(s): 12.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.5\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3436
Affected Version(s): 12.5\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.6\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.6\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3439
Affected Version(s): 12.7\\(1\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3440
Affected Version(s): 12.7\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.8\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.8\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3443
Affected Version(s): 12.8\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 14.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 14.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3447
Affected Version(s): 14.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3450
Affected Version(s): 9.3\\(3\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3451
Affected Version(s): 9.3\\(4\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3454
Affected Version(s): 9.3\\(4\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Product: ip_phone_8845_firmware					
Affected Version(s): 10.1\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.1\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3458
Affected Version(s): 10.2\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-IP_P-201222/3459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.2\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.2\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 10.3\\(1.11\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3462
Affected Version(s): 10.3\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3465
Affected Version(s): 10.3\\(1\\)sr2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3466
Affected Version(s): 10.3\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr4					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr4b					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3469
Affected Version(s): 10.3\\(1\\)sr5					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.3\\(1\\)sr6					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr7					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 10.3\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3473
Affected Version(s): 10.4\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.4\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11-0-1msr1-1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3476
Affected Version(s): 11.0\\(0.7\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3477
Affected Version(s): 11.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3480
Affected Version(s): 11.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3484
Affected Version(s): 12.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3487
Affected Version(s): 12.5\\(1\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3488
Affected Version(s): 12.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3491
Affected Version(s): 12.6\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.6\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.7\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3495
Affected Version(s): 12.8\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.8\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.8\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3498
Affected Version(s): 14.0\\(1\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3499
Affected Version(s): 14.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3502
Affected Version(s): 14.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 14.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(3\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 9.3\\(4\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3506
Affected Version(s): 9.3\\(4\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3509
Product: ip_phone_8851_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 10.1\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3510
Affected Version(s): 10.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.1\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.2\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3513
Affected Version(s): 10.2\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of	https://tools.cisco.com/security/center/	O-CIS-IP_P-201222/3514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	content/Cisco SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.2\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1.11\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3517
Affected Version(s): 10.3\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-IP_P-201222/3518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.3\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 10.3\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3521
Affected Version(s): 10.3\\(1\\)sr4					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr4b					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr5					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3524
Affected Version(s): 10.3\\(1\\)sr6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3525
Affected Version(s): 10.3\\(1\\)sr7					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.4\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3528
Affected Version(s): 10.4\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 11-0-1msr1-1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.0\\(0.7\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 11.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3532
Affected Version(s): 11.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3535
Affected Version(s): 12.0\\(1\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3536
Affected Version(s): 12.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3539
Affected Version(s): 12.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3543
Affected Version(s): 12.5\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.6\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3546
Affected Version(s): 12.6\\(1\\)sr1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3547
Affected Version(s): 12.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.7\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.8\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3550
Affected Version(s): 12.8\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.8\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 14.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3554
Affected Version(s): 14.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3557
Affected Version(s): 14.1\\(1\\)sr1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3558
Affected Version(s): 9.3\\(3\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3561
Affected Version(s): 9.3\\(4\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 9.3\\(4\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Product: ip_phone_8861_firmware					
Affected Version(s): 10.1\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3565
Affected Version(s): 10.1\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-IP_P-201222/3566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.2\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.2\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 10.2\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3569
Affected Version(s): 10.3\\(1.11\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3572
Affected Version(s): 10.3\\(1\\)sr1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3573
Affected Version(s): 10.3\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr4					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3576
Affected Version(s): 10.3\\(1\\)sr4b					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.3\\(1\\)sr5					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr6					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 10.3\\(1\\)sr7					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3580
Affected Version(s): 10.3\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.4\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.4\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3583
Affected Version(s): 11-0-1msr1-1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3584
Affected Version(s): 11.0\\(0.7\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3587
Affected Version(s): 11.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 11.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3591
Affected Version(s): 12.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3594
Affected Version(s): 12.1\\(1\\)sr1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3595
Affected Version(s): 12.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3598
Affected Version(s): 12.5\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.6\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.6\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3602
Affected Version(s): 12.7\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.8\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.8\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3605
Affected Version(s): 12.8\\(1\\)sr2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3606
Affected Version(s): 14.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3609
Affected Version(s): 14.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 14.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 9.3\\(3\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3613
Affected Version(s): 9.3\\(4\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3616
Affected Version(s): 9.3\\(4\\)sr3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3617
Product: ip_phone_8865_firmware					
Affected Version(s): 10.1\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.1\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3620
Affected Version(s): 10.2\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of	https://tools.cisco.com/security/center/	O-CIS-IP_P-201222/3621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	content/Cisco SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.2\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.2\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1.11\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3624
Affected Version(s): 10.3\\(1.9\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-IP_P-201222/3625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.3\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 10.3\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3628
Affected Version(s): 10.3\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr4					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr4b					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3631
Affected Version(s): 10.3\\(1\\)sr5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3632
Affected Version(s): 10.3\\(1\\)sr6					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(1\\)sr7					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 10.3\\(2\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3635
Affected Version(s): 10.4\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 10.4\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11-0-1msr1-1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 11.0\\(0.7\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3639
Affected Version(s): 11.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 11.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3642
Affected Version(s): 11.7\\(1\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3643
Affected Version(s): 12.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3646
Affected Version(s): 12.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.1\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 12.5\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3650
Affected Version(s): 12.5\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.5\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3653
Affected Version(s): 12.6\\(1\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3654
Affected Version(s): 12.6\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.7\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.7\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3657
Affected Version(s): 12.8\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 12.8\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 12.8\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Affected Version(s): 14.0\\(1\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3661
Affected Version(s): 14.0\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 14.0\\(1\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3664
Affected Version(s): 14.1\\(1\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3665
Affected Version(s): 14.1\\(1\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(3\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3668
Affected Version(s): 9.3\\(4\\)sr1					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and	https://tools.cisco.com/security/center/content/Cisco	O-CIS-IP_P-201222/3669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**	SecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	
Affected Version(s): 9.3\\(4\\)sr2					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. **CVE ID : CVE-2022-20968**		
Affected Version(s): 9.3\\(4\\)sr3					
Out-of-bounds Write	12-Dec-2022	8.8	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U	O-CIS-IP_P-201222/3671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20968		
Vendor: Citrix					
Product: application_delivery_controller_firmware					
Affected Version(s): From (including) 12.1 Up to (excluding) 12.1-55.291					
N/A	13-Dec-2022	9.8	Unauthenticated remote arbitrary code execution **CVE ID : CVE-2022-27518**	https://support.citrix.com/article/CTX474995	O-CIT-APPL-201222/3672
Affected Version(s): From (including) 12.1 Up to (excluding) 12.1-65.25					
N/A	13-Dec-2022	9.8	Unauthenticated remote arbitrary code execution **CVE ID : CVE-2022-27518**	https://support.citrix.com/article/CTX474995	O-CIT-APPL-201222/3673
Affected Version(s): From (including) 13.0 Up to (excluding) 13.0-58.32					
N/A	13-Dec-2022	9.8	Unauthenticated remote arbitrary code execution **CVE ID : CVE-2022-27518**	https://support.citrix.com/article/CTX474995	O-CIT-APPL-201222/3674
Product: gateway_firmware					
Affected Version(s): From (including) 12.1 Up to (excluding) 12.1-65.25					
N/A	13-Dec-2022	9.8	Unauthenticated remote arbitrary code execution **CVE ID : CVE-2022-27518**	https://support.citrix.com/article/CTX474995	O-CIT-GATE-201222/3675
Affected Version(s): From (including) 13.0 Up to (excluding) 13.0-58.32					
N/A	13-Dec-2022	9.8	Unauthenticated remote arbitrary code execution **CVE ID : CVE-2022-27518**	https://support.citrix.com/article/CTX474995	O-CIT-GATE-201222/3676
Vendor: D-link					
Product: dhp-w310av_firmware					
Affected Version(s): 3.10eu					
Improper Neutralization of	02-Dec-2022	9.8	D-Link DHP-W310AV 3.10EU was discovered to contain a command	N/A	O-D-L-DHP--201222/3677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			injection vulnerability via the System Checks function. **CVE ID : CVE-2022-44930**		
Product: dvg-g5402sp_firmware					
Affected Version(s): ge_1.03					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	9.8	D-Link DVG-G5402SP GE_1.03 was discovered to contain a command injection vulnerability via the Maintenance function. **CVE ID : CVE-2022-44928**	N/A	O-D-L-DVG--201222/3678
Improper Privilege Management	02-Dec-2022	9.8	An access control issue in D-Link DVG-G5402SP GE_1.03 allows unauthenticated attackers to escalate privileges via arbitrarily editing VoIP SIB profiles. **CVE ID : CVE-2022-44929**	N/A	O-D-L-DVG--201222/3679
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Dec-2022	6.1	AWStats 7.x through 7.8 allows XSS in the hostinfo plugin due to printing a response from Net::XWhois without proper checks. **CVE ID : CVE-2022-46391**	https://github.com/eldy/AWStats/pull/226	O-DEB-DEBI-201222/3680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 11.0					
Integer Overflow or Wraparound	06-Dec-2022	7.8	An integer overflow in the VNC module in VideoLAN VLC Media Player through 3.0.17.4 allows attackers, by tricking a user into opening a crafted playlist or connecting to a rogue VNC server, to crash VLC or execute code under some conditions. **CVE ID : CVE-2022-41325**	https://www.videolan.org/security/sb-vlc3018.html, https://www.synacktiv.com/sites/default/files/2022-11/vlc_vnc_int_overflow-CVE-2022-41325.pdf	O-DEB-DEBI-201222/3681
Vendor: digitalalertsystems					
Product: dasdec_iii_firmware					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-2022	5.4	A cross-site scripting (XSS) vulnerability exists in all current versions of Digital Alert Systems DASDEC software via the Host Header in undisclosed pages after login. **CVE ID : CVE-2022-40204**	https://www.digitalalertsystems.com/security-advisory	O-DIG-DASD-201222/3682
Product: dasdec_ii_firmware					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-2022	5.4	A cross-site scripting (XSS) vulnerability exists in all current versions of Digital Alert Systems DASDEC software via the Host Header in undisclosed pages after login. **CVE ID : CVE-2022-40204**	https://www.digitalalertsystems.com/security-advisory	O-DIG-DASD-201222/3683
Product: dasdec_i_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-2022	5.4	A cross-site scripting (XSS) vulnerability exists in all current versions of Digital Alert Systems DASDEC software via the Host Header in undisclosed pages after login. **CVE ID : CVE-2022-40204**	https://www.digitalalertsystems.com/security-advisory	O-DIG-DASD-201222/3684
Product: one-net_firmware					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-2022	5.4	A cross-site scripting (XSS) vulnerability exists in all current versions of Digital Alert Systems DASDEC software via the Host Header in undisclosed pages after login. **CVE ID : CVE-2022-40204**	https://www.digitalalertsystems.com/security-advisory	O-DIG-ONE--201222/3685
Product: one-net_se_firmware					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-2022	5.4	A cross-site scripting (XSS) vulnerability exists in all current versions of Digital Alert Systems DASDEC software via the Host Header in undisclosed pages after login. **CVE ID : CVE-2022-40204**	https://www.digitalalertsystems.com/security-advisory	O-DIG-ONE--201222/3686
Vendor: dragino					
Product: lg01_lora_firmware					
Affected Version(s): 4.3.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Files or Directories Accessible to External Parties	12-Dec-2022	7.5	The web portal of Dragino Lora LG01 18ed40 IoT v4.3.4 has the directory listing at the URL https://10.10.20.74/lib/. This address has a backup file which can be downloaded without any authentication. **CVE ID : CVE-2022-45227**	N/A	O-DRA-LG01-201222/3687
Cross-Site Request Forgery (CSRF)	12-Dec-2022	3.5	Dragino Lora LG01 18ed40 IoT v4.3.4 was discovered to contain a Cross-Site Request Forgery in the logout page. **CVE ID : CVE-2022-45228**	N/A	O-DRA-LG01-201222/3688
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 35					
Improper Link Resolution Before File Access ('Link Following')	08-Dec-2022	5.3	A vulnerability was found in buildah. Incorrect following of symlinks while reading .containerignore and .dockerignore results in information disclosure. **CVE ID : CVE-2022-4122**	https://github.com/containers/podman/pull/16315	O-FED-FEDO-201222/3689
Relative Path Traversal	08-Dec-2022	3.3	A flaw was found in Buildah. The local path and the lowest subdirectory may be disclosed due to incorrect absolute path traversal, resulting in an impact to confidentiality.	N/A	O-FED-FEDO-201222/3690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-4123		
Affected Version(s): 36					
Improper Link Resolution Before File Access ('Link Following')	08-Dec-2022	5.3	A vulnerability was found in buildah. Incorrect following of symlinks while reading .containerignore and .dockerignore results in information disclosure. **CVE ID : CVE-2022-4122**	https://github.com/containers/podman/pull/16315	O-FED-FEDO-201222/3691
Relative Path Traversal	08-Dec-2022	3.3	A flaw was found in Buildah. The local path and the lowest subdirectory may be disclosed due to incorrect absolute path traversal, resulting in an impact to confidentiality. **CVE ID : CVE-2022-4123**	N/A	O-FED-FEDO-201222/3692
Affected Version(s): 37					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	09-Dec-2022	9.8	The rxvt-unicode package is vulnerable to a remote code execution, in the Perl background extension, when an attacker can control the data written to the user's terminal and certain options are set. **CVE ID : CVE-2022-4170**	N/A	O-FED-FEDO-201222/3693
Improper Link Resolution Before File Access	08-Dec-2022	5.3	A vulnerability was found in buildah. Incorrect following of symlinks while reading .containerignore and	https://github.com/containers/podman/pull/16315	O-FED-FEDO-201222/3694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Link Following')			.dockerignore results in information disclosure. **CVE ID : CVE-2022-4122**		
Relative Path Traversal	08-Dec-2022	3.3	A flaw was found in Buildah. The local path and the lowest subdirectory may be disclosed due to incorrect absolute path traversal, resulting in an impact to confidentiality. **CVE ID : CVE-2022-4123**	N/A	O-FED-FEDO-201222/3695
Vendor: Festo					
Product: bus_module_cpx-e-ep_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-BUS_-201222/3696
Product: bus_node_cpx-fb32_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-BUS_-201222/3697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: bus_node_cpx-fb33_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-BUS_-201222/3698
Product: bus_node_cpx-fb36_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-BUS_-201222/3699
Product: bus_node_cpx-fb37_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-BUS_-201222/3700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: bus_node_cpx-fb39_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-BUS_-201222/3701
Product: bus_node_cpx-fb40_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-BUS_-201222/3702
Product: bus_node_cpx-fb43_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-BUS_-201222/3703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: bus_node_cpx-m-fb34_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-BUS_-201222/3704
Product: bus_node_cpx-m-fb35_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-BUS_-201222/3705
Product: bus_node_cpx-m-fb44_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-BUS_-201222/3706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: bus_node_cpx-m-fb45_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-BUS_-201222/3707
Product: bus_node_cteu-ep_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-BUS_-201222/3708
Product: bus_node_cteu-pn-ex1c_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-BUS_-201222/3709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: bus_node_cteu-pn_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-BUS_-201222/3710
Product: camera_system_chb-c-n_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-CAME-201222/3711
Product: cecx-x-c1_modular_master_controller_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-CECX-201222/3712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: cecx-x-m1_modular_controller_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-CECX-201222/3713
Product: compact_vision_system_sboc-c_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-COMP-201222/3714
Product: compact_vision_system_sboc-m_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-COMP-201222/3715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: compact_vision_system_sboc-q_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-COMP-201222/3716
Product: compact_vision_system_sboi-c_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-COMP-201222/3717
Product: compact_vision_system_sboi-m_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-COMP-201222/3718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: compact_vision_system_sboi-q_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-COMP-201222/3719
Product: controller_cecc-d-ba_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-CONT-201222/3720
Product: controller_cecc-d_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-CONT-201222/3721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: controller_cecc-lk_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-CONT-201222/3722
Product: controller_cecc-s_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-CONT-201222/3723
Product: controller_cecc-x-m1-mv-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-CONT-201222/3724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: controller_cecc-x-m1-mv_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-CONT-201222/3725
Product: controller_cecc-x-m1-y-yjkp_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-CONT-201222/3726
Product: controller_cecc-x-m1-ys-l1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-CONT-201222/3727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: controller_cecc-x-m1-ys-l2_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-CONT-201222/3728
Product: controller_cecc-x-m1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-CONT-201222/3729
Product: controller_cmxh-st2-c5-7-diop_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-CONT-201222/3730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: controller_sbrd-q_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-CONT-201222/3731
Product: control_block_cpx-cec-c1-v3_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-CONT-201222/3732
Product: control_block_cpx-cec-c1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-CONT-201222/3733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: control_block_cpx-cec-m1-v3_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-CONT-201222/3734
Product: control_block_cpx-cec-m1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-CONT-201222/3735
Product: control_block_cpx-cec-s1-v3_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-CONT-201222/3736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: control_block_cpx-cec_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-CONT-201222/3737
Product: control_block_cpx-cmxx_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-CONT-201222/3738
Product: control_block_cpx-fec-1-ie_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-CONT-201222/3739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: ethernet\/ip_interface_cpx-ap-i-ep-m12_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-ETHE-201222/3740
Product: ethernet\/ip_interface_cpx-ap-i-pn-m12_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-ETHE-201222/3741
Product: gateway_cpx-iot_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-GATE-201222/3742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: integrated_drive_emca-ec-67-m-1te-ep_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-INTE-201222/3743
Product: integrated_drive_emca-ec-67_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-INTE-201222/3744
Product: motor_controller_cmmo-st-c5-1-dion_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-MOTO-201222/3745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: motor_controller_cmmo-st-c5-1-diop_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-MOTO-201222/3746
Product: motor_controller_cmmo-st-c5-1-lkp_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-MOTO-201222/3747
Product: motor_controller_cmmp-as-c10-11a-p3-m0_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-MOTO-201222/3748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: motor_controller_cmmp-as-c10-11a-p3-m3_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-MOTO-201222/3749
Product: motor_controller_cmmp-as-c15-11a-p3-m3_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-MOTO-201222/3750
Product: motor_controller_cmmp-as-c2-3a-m0_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-MOTO-201222/3751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: motor_controller_cmmp-as-c2-3a-m3_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-MOTO-201222/3752
Product: motor_controller_cmmp-as-c5-11a-p3-m0_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-MOTO-201222/3753
Product: motor_controller_cmmp-as-c5-11a-p3-m3_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-MOTO-201222/3754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: motor_controller_cmmp-as-c5-3a-m0_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-MOTO-201222/3755
Product: motor_controller_cmmp-as-c5-3a-m3_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-MOTO-201222/3756
Product: operator_unit_cdpx-x-a-s-10_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-OPER-201222/3757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: operator_unit_cdpx-x-a-w-13_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-OPER-201222/3758
Product: operator_unit_cdpx-x-a-w-4_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-OPER-201222/3759
Product: operator_unit_cdpx-x-a-w-7_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-OPER-201222/3760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: planar_surface_gantry_excm-30_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-PLAN-201222/3761
Product: planar_surface_gantry_excm-40_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-PLAN-201222/3762
Product: servo_cmmt-as-c12-11a-p3-ec-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-SERV-201222/3763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: servo_cmmt-as-c12-11a-p3-ep-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3764
Product: servo_cmmt-as-c12-11a-p3-mp-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3765
Product: servo_cmmt-as-c12-11a-p3-pn-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-SERV-201222/3766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: servo_cmmt-as-c2-11a-p3-ec-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3767
Product: servo_cmmt-as-c2-11a-p3-ep-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3768
Product: servo_cmmt-as-c2-11a-p3-mp-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-SERV-201222/3769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: servo_cmmt-as-c2-11a-p3-pn-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3770
Product: servo_cmmt-as-c2-3a-ec-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3771
Product: servo_cmmt-as-c2-3a-ep-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-SERV-201222/3772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: servo_cmmt-as-c2-3a-mp-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3773
Product: servo_cmmt-as-c2-3a-pn-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3774
Product: servo_cmmt-as-c3-11a-p3-ec-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-SERV-201222/3775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: servo_cmmt-as-c3-11a-p3-ep-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3776
Product: servo_cmmt-as-c3-11a-p3-mp-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3777
Product: servo_cmmt-as-c3-11a-p3-pn-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-SERV-201222/3778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: servo_cmmt-as-c4-3a-ec-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3779
Product: servo_cmmt-as-c4-3a-ep-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3780
Product: servo_cmmt-as-c4-3a-mp-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-SERV-201222/3781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: servo_cmmt-as-c4-3a-pn-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3782
Product: servo_cmmt-as-c5-11a-p3-ec-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3783
Product: servo_cmmt-as-c5-11a-p3-ep-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-SERV-201222/3784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: servo_cmmt-as-c5-11a-p3-mp-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3785
Product: servo_cmmt-as-c5-11a-p3-pn-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3786
Product: servo_cmmt-as-c7-11a-p3-ec-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-SERV-201222/3787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: servo_cmmt-as-c7-11a-p3-ep-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3788
Product: servo_cmmt-as-c7-11a-p3-mp-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3789
Product: servo_cmmt-as-c7-11a-p3-pn-s1_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-SERV-201222/3790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: servo_drive_cmmt-st-c8-1c-ep-s0_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3791
Product: servo_drive_cmmt-st-c8-1c-pn-s0_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-SERV-201222/3792
Product: vtem-s1-27_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability.	N/A	O-FES-VTEM-201222/3793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3270		
Product: vtem-s1-c_firmware					
Affected Version(s): -					
N/A	01-Dec-2022	9.8	In multiple products by Festo a remote unauthenticated attacker could use functions of an undocumented protocol which could lead to a complete loss of confidentiality, integrity and availability. **CVE ID : CVE-2022-3270**	N/A	O-FES-VTEM-201222/3794
Vendor: flir					
Product: flir_ax8_firmware					
Affected Version(s): From (including) 1.46.0 Up to (excluding) 1.46.16					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Dec-2022	9.8	A vulnerability classified as critical has been found in Teledyne FLIR AX8 up to 1.46.16. Affected is an unknown function of the file palette.php of the component Web Service Handler. The manipulation of the argument palette leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-215118 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4364**	N/A	O-FLI-FLIR-201222/3795
Vendor: force1rc					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: discovery_wifi_u818a_hd\+_fpv_firmware					
Affected Version(s): 2.0.10					
Out-of-bounds Write	06-Dec-2022	9.8	Buffer overflow in firmware lewei_cam binary version 2.0.10 in Force 1 Discovery Wifi U818A HD+ FPV Drone allows attacker to gain remote code execution as root user via a specially crafted UDP packet. Please update the Reference section to these links > http://thiscomputer.com/ > https://www.bostoncyber.org/ > https://medium.com/@meekworth/exploiting-the-lw9621-drone-camera-module-773f00081368 **CVE ID : CVE-2022-40918**	N/A	O-FOR-DISC-201222/3796
Vendor: Fortinet					
Product: fortios					
Affected Version(s): 7.2.0					
N/A	06-Dec-2022	9.8	An authentication bypass by assumed-immutable data vulnerability [CWE-302] in the FortiOS SSH login component 7.2.0, 7.0.0 through 7.0.7, 6.4.0 through 6.4.9, 6.2 all versions, 6.0 all versions and FortiProxy SSH login component 7.0.0 through 7.0.5, 2.0.0 through 2.0.10, 1.2.0 all versions may allow a remote and unauthenticated attacker	https://fortiguard.com/psirt/FG-IR-22-255	O-FOR-FORT-201222/3797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to login into the device via sending specially crafted Access-Challenge response from the Radius server. **CVE ID : CVE-2022-35843**		
Affected Version(s): 7.2.1					
N/A	06-Dec-2022	9.8	An authentication bypass by assumed-immutable data vulnerability [CWE-302] in the FortiOS SSH login component 7.2.0, 7.0.0 through 7.0.7, 6.4.0 through 6.4.9, 6.2 all versions, 6.0 all versions and FortiProxy SSH login component 7.0.0 through 7.0.5, 2.0.0 through 2.0.10, 1.2.0 all versions may allow a remote and unauthenticated attacker to login into the device via sending specially crafted Access-Challenge response from the Radius server. **CVE ID : CVE-2022-35843**	https://fortiguard.com/psirt/FG-IR-22-255	O-FOR-FORT-201222/3798
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.15					
N/A	06-Dec-2022	9.8	An authentication bypass by assumed-immutable data vulnerability [CWE-302] in the FortiOS SSH login component 7.2.0, 7.0.0 through 7.0.7, 6.4.0 through 6.4.9, 6.2 all versions, 6.0 all versions and FortiProxy SSH login component 7.0.0 through 7.0.5, 2.0.0 through 2.0.10, 1.2.0 all versions	https://fortiguard.com/psirt/FG-IR-22-255	O-FOR-FORT-201222/3799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow a remote and unauthenticated attacker to login into the device via sending specially crafted Access-Challenge response from the Radius server. **CVE ID : CVE-2022-35843**		
Affected Version(s): From (including) 6.0.7 Up to (including) 6.0.15					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	5.4	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiOS 6.0.7 - 6.0.15, 6.2.2 - 6.2.12, 6.4.0 - 6.4.9 and 7.0.0 - 7.0.3 allows a privileged attacker to execute unauthorized code or commands via storing malicious payloads in replacement messages. **CVE ID : CVE-2022-40680**	https://fortiguard.com/psirt/FG-IR-21-248	O-FOR-FORT-201222/3800
Affected Version(s): From (including) 6.2.0 Up to (including) 6.2.12					
N/A	06-Dec-2022	9.8	An authentication bypass by assumed-immutable data vulnerability [CWE-302] in the FortiOS SSH login component 7.2.0, 7.0.0 through 7.0.7, 6.4.0 through 6.4.9, 6.2 all versions, 6.0 all versions and FortiProxy SSH login component 7.0.0 through 7.0.5, 2.0.0 through 2.0.10, 1.2.0 all versions may allow a remote and unauthenticated attacker to login into the device	https://fortiguard.com/psirt/FG-IR-22-255	O-FOR-FORT-201222/3801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via sending specially crafted Access-Challenge response from the Radius server. **CVE ID : CVE-2022-35843**		
Affected Version(s): From (including) 6.2.2 Up to (including) 6.2.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	5.4	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiOS 6.0.7 - 6.0.15, 6.2.2 - 6.2.12, 6.4.0 - 6.4.9 and 7.0.0 - 7.0.3 allows a privileged attacker to execute unauthorized code or commands via storing malicious payloads in replacement messages. **CVE ID : CVE-2022-40680**	https://fortiguard.com/psirt/FG-IR-21-248	O-FOR-FORT-201222/3802
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.9					
N/A	06-Dec-2022	9.8	An authentication bypass by assumed-immutable data vulnerability [CWE-302] in the FortiOS SSH login component 7.2.0, 7.0.0 through 7.0.7, 6.4.0 through 6.4.9, 6.2 all versions, 6.0 all versions and FortiProxy SSH login component 7.0.0 through 7.0.5, 2.0.0 through 2.0.10, 1.2.0 all versions may allow a remote and unauthenticated attacker to login into the device via sending specially crafted Access-Challenge	https://fortiguard.com/psirt/FG-IR-22-255	O-FOR-FORT-201222/3803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response from the Radius server. **CVE ID : CVE-2022-35843**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	5.4	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiOS 6.0.7 - 6.0.15, 6.2.2 - 6.2.12, 6.4.0 - 6.4.9 and 7.0.0 - 7.0.3 allows a privileged attacker to execute unauthorized code or commands via storing malicious payloads in replacement messages. **CVE ID : CVE-2022-40680**	https://fortiguard.com/psirt/FG-IR-21-248	O-FOR-FORT-201222/3804
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	5.4	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiOS 6.0.7 - 6.0.15, 6.2.2 - 6.2.12, 6.4.0 - 6.4.9 and 7.0.0 - 7.0.3 allows a privileged attacker to execute unauthorized code or commands via storing malicious payloads in replacement messages. **CVE ID : CVE-2022-40680**	https://fortiguard.com/psirt/FG-IR-21-248	O-FOR-FORT-201222/3805
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.7					
N/A	06-Dec-2022	9.8	An authentication bypass by assumed-immutable data vulnerability [CWE-	https://fortiguard.com/psir	O-FOR-FORT-201222/3806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			302] in the FortiOS SSH login component 7.2.0, 7.0.0 through 7.0.7, 6.4.0 through 6.4.9, 6.2 all versions, 6.0 all versions and FortiProxy SSH login component 7.0.0 through 7.0.5, 2.0.0 through 2.0.10, 1.2.0 all versions may allow a remote and unauthenticated attacker to login into the device via sending specially crafted Access-Challenge response from the Radius server. **CVE ID : CVE-2022-35843**	t/FG-IR-22-255	
Vendor: Franklinfueling					
Product: colibri_firmware					
Affected Version(s): 1.9.22.8925					
Incorrect Authorization	05-Dec-2022	9.8	Franklin Fueling System FFS Colibri 1.9.22.8925 is affected by: File system overwrite. The impact is: File system rewrite (remote). ¶¶ An attacker can overwrite system files like [system.conf] and [passwd], this occurs because the insecure usage of "fopen" system function with the mode "wb" which allows overwriting file if exists. Overwriting files such as passwd, allows an attacker to escalate his privileges by planting backdoor user with root privilege or change root password.	N/A	O-FRA-COLI-201222/3807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-44039		
Vendor: fsi					
Product: fs020w_firmware					
Affected Version(s): * Up to (including) 4.0.0					
Cross-Site Request Forgery (CSRF)	05-Dec-2022	7.3	Cross-site request forgery (CSRF) vulnerability in +F FS040U software versions v2.3.4 and earlier, +F FS020W software versions v4.0.0 and earlier, +F FS030W software versions v3.3.5 and earlier, and +F FS040W software versions v1.4.1 and earlier allows an adjacent attacker to hijack the authentication of an administrator and user's unintended operations such as to reboot the product and/or reset the configuration to the initial set-up may be performed. **CVE ID : CVE-2022-43470**	https://www.fsi.co.jp/mobile/plusF/news/22102803.html, https://www.fsi.co.jp/mobile/plusF/news/22102802.html, https://www.fsi.co.jp/mobile/plusF/news/22102804.html, https://www.fsi.co.jp/mobile/plusF/news/22102801.html	O-FSI-FS02-201222/3808
Product: fs030w_firmware					
Affected Version(s): * Up to (including) 3.3.5					
Cross-Site Request Forgery (CSRF)	05-Dec-2022	7.3	Cross-site request forgery (CSRF) vulnerability in +F FS040U software versions v2.3.4 and earlier, +F FS020W software versions v4.0.0 and earlier, +F FS030W software versions v3.3.5	https://www.fsi.co.jp/mobile/plusF/news/22102803.html, https://www.fsi.co.jp/mobile/plusF/news/22102802.ht	O-FSI-FS03-201222/3809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, and +F FS040W software versions v1.4.1 and earlier allows an adjacent attacker to hijack the authentication of an administrator and user's unintended operations such as to reboot the product and/or reset the configuration to the initial set-up may be performed. **CVE ID : CVE-2022-43470**	ml, https://www.fsi.co.jp/mobile/plusF/news/22102804.html, https://www.fsi.co.jp/mobile/plusF/news/22102801.html	
Product: fs040u_firmware					
Affected Version(s): * Up to (including) 2.3.4					
Cross-Site Request Forgery (CSRF)	05-Dec-2022	7.3	Cross-site request forgery (CSRF) vulnerability in +F FS040U software versions v2.3.4 and earlier, +F FS020W software versions v4.0.0 and earlier, +F FS030W software versions v3.3.5 and earlier, and +F FS040W software versions v1.4.1 and earlier allows an adjacent attacker to hijack the authentication of an administrator and user's unintended operations such as to reboot the product and/or reset the configuration to the initial set-up may be performed.	https://www.fsi.co.jp/mobile/plusF/news/22102803.html, https://www.fsi.co.jp/mobile/plusF/news/22102802.html, https://www.fsi.co.jp/mobile/plusF/news/22102804.html, https://www.fsi.co.jp/mobile/plusF/news/22102801.html	O-FSI-FS04-201222/3810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43470		
Insufficiently Protected Credentials	05-Dec-2022	4.6	Plaintext storage of a password vulnerability exists in +F FS040U software versions v2.3.4 and earlier, which may allow an attacker to obtain the login password of +F FS040U and log in to the management console. **CVE ID : CVE-2022-43442**	https://www.fsi.co.jp/mobile/plusF/news/22102803.html, https://www.fsi.co.jp/mobile/plusF/news/22102802.html, https://www.fsi.co.jp/mobile/plusF/news/22102804.html, https://www.fsi.co.jp/mobile/plusF/news/22102801.html	O-FSI-FS04-201222/3811
Product: fs040w_firmware					
Affected Version(s): * Up to (including) 1.4.1					
Cross-Site Request Forgery (CSRF)	05-Dec-2022	7.3	Cross-site request forgery (CSRF) vulnerability in +F FS040U software versions v2.3.4 and earlier, +F FS020W software versions v4.0.0 and earlier, +F FS030W software versions v3.3.5 and earlier, and +F FS040W software versions v1.4.1 and earlier allows an adjacent attacker to hijack the authentication of an administrator and user's unintended operations such as to reboot the product	https://www.fsi.co.jp/mobile/plusF/news/22102803.html, https://www.fsi.co.jp/mobile/plusF/news/22102802.html, https://www.fsi.co.jp/mobile/plusF/news/22102804.html, https://www.fsi.co.jp/mobile/plusF/news	O-FSI-FS04-201222/3812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and/or reset the configuration to the initial set-up may be performed. **CVE ID : CVE-2022-43470**	/22102801.html	
Vendor: Google					
Product: android					
Affected Version(s): 10.0					
Out-of-bounds Read	13-Dec-2022	9.8	In toLanguageTag of LocaleListCache.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239210579 **CVE ID : CVE-2022-20472**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3813
Out-of-bounds Read	13-Dec-2022	9.8	In toLanguageTag of LocaleListCache.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-239267173 **CVE ID : CVE-2022-20473**		
Out-of-bounds Write	13-Dec-2022	8.8	In avdt_msg_asmbl of avdt_msg.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-232023771 **CVE ID : CVE-2022-20411**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3815
Out-of-bounds Write	13-Dec-2022	8.8	In avct_lcb_msg_asmbl of avct_lcb_act.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230867224 **CVE ID : CVE-2022-20469**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39097**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3817
Integer Overflow or Wraparound	08-Dec-2022	7.8	Integer overflow vulnerability in Samsung decoding library for video thumbnails prior to SMR Dec-2022 Release 1 allows local attacker to perform Out-Of-Bounds Write. **CVE ID : CVE-2022-39907**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3818
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39101**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3819
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39098**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Dec-2022	7.8	In bindRemoteViewsService of AppWidgetServiceImpl.java, there is a possible way to bypass background activity launch 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-10 Android-11 Android-12 Android-12L Android-13Android ID: A-234013191 **CVE ID : CVE-2022-20470**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3821
N/A	13-Dec-2022	7.8	In readLazyValue of Parcel.java, there is a possible loading of arbitrary code into the System Settings app due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-240138294 **CVE ID : CVE-2022-20474**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39099**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3823
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-241764135 **CVE ID : CVE-2022-20478**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3824
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-12 Android-12L Android-13Android ID: A-241764340 **CVE ID : CVE-2022-20479**		
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-241764350 **CVE ID : CVE-2022-20480**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3826
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39100**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3827
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242702851 **CVE ID : CVE-2022-20484**		
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242702935 **CVE ID : CVE-2022-20485**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3829
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. 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/2022-12-01	O-GOO-ANDR-201222/3830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242703118 **CVE ID : CVE-2022-20486**		
Missing Authorization	06-Dec-2022	7.8	In UscAIEngine service, there is a missing permission check. This could lead to set up UscAIEngine service with no additional execution privileges needed. **CVE ID : CVE-2022-42776**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3831
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-42777**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3832
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39102**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3833
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no	https://www.unisoc.com/en_us/secy/announcementDetail/159958	O-GOO-ANDR-201222/3834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. **CVE ID : CVE-2022-39090**	806098841100 6	
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39091**	https://www.unisoc.com/en_us/secy/announcementDetail/159958806098841100 6	O-GOO-ANDR-201222/3835
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39092**	https://www.unisoc.com/en_us/secy/announcementDetail/159958806098841100 6	O-GOO-ANDR-201222/3836
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39093**	https://www.unisoc.com/en_us/secy/announcementDetail/159958806098841100 6	O-GOO-ANDR-201222/3837
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no	https://www.unisoc.com/en_us/secy/announcementDetail/159958806098841100 6	O-GOO-ANDR-201222/3838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. **CVE ID : CVE-2022-39094**		
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39095**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3839
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39096**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3840
Integer Overflow or Wraparound	13-Dec-2022	7.5	In several functions that parse avrc response in avrc_pars_ct.cc and related files, there are possible out of bounds reads due to integer overflows. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-242459126 **CVE ID : CVE-2022-20483**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Dec-2022	7.4	TOCTOU vulnerability in Samsung decoding library for video thumbnails prior to SMR Dec-2022 Release 1 allows local attacker to perform Out-Of-Bounds Write. **CVE ID : CVE-2022-39908**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3842
Improper Restriction of Rendered UI Layers or Frames	13-Dec-2022	7.3	In onCreate of ReviewPermissionsActivity.java, there is a possible way to grant permissions for a separate app with API level < 23 due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-176094367 **CVE ID : CVE-2022-20442**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3843
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/3844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/3845
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/3846
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/3847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**		
Out-of-bounds Write	05-Dec-2022	6.7	In mpu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07541753; Issue ID: ALPS07541753. **CVE ID : CVE-2022-32620**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/3848
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/3849
Out-of-bounds Read	13-Dec-2022	6.5	In BNEP_ConnectResp of bnep_api.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure over	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-228450451 **CVE ID : CVE-2022-20468**		
Out-of-bounds Write	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39129**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3851
Out-of-bounds Read	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39130**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3852
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39131**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3853
Out-of-bounds Write	06-Dec-2022	5.5	In camera driver, there is a possible out of bounds write due to a missing	https://www.unisoc.com/en_us/secy/an	O-GOO-ANDR-201222/3854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39132**	nouncementDetail/15995880609884110 06	
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-39133**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3855
Insertion of Sensitive Information into Log File	08-Dec-2022	5.5	Exposure of Sensitive Information vulnerability in kernel prior to SMR Dec-2022 Release 1 allows attackers to access the kernel address information via log. **CVE ID : CVE-2022-39897**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3856
N/A	08-Dec-2022	5.5	Implicit intent hijacking vulnerability in Telecom application prior to SMR Dec-2022 Release 1 allows attacker to access sensitive information via implicit intent. **CVE ID : CVE-2022-39905**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3857
Insecure Default Initialization of Resource	13-Dec-2022	5.5	In applyKeyguardFlags of NotificationShadeWindowControllerImpl.java, there is a possible way to observe the user's password on a secondary display due to an insecure default value. This could lead to local information disclosure with no additional	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-179725730 **CVE ID : CVE-2022-20466**		
N/A	08-Dec-2022	5.5	Improper access control vulnerability in Calendar prior to versions 11.6.08.0 in Android Q(10), 12.2.11.3000 in Android R(11), 12.3.07.2000 in Android S(12), and 12.4.02.0 in Android T(13) allows attackers to access sensitive information via implicit intent. **CVE ID : CVE-2022-39915**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=12	O-GOO-ANDR-201222/3859
Use After Free	06-Dec-2022	5.5	In npu driver, there is a memory corruption due to a use after free. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42754**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3860
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42755**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3861
Buffer Copy	06-Dec-2022	5.5	In sensor driver, there is a possible buffer	https://www.unisoc.com/e	O-GOO-ANDR-201222/3862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			overflow due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42756**	n_us/secy/announcementDetail/15995880609884110 06	
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42759**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3863
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42760**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3864
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42761**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3865
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42762**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3866
Integer Overflow or	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to	https://www.unisoc.com/en_us/secy/announcementD	O-GOO-ANDR-201222/3867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			local denial of service in wlan services. **CVE ID : CVE-2022-42763**	etail/15995880609884110 06	
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42764**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3868
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42765**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3869
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42766**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3870
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42782**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3871
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42772**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42773**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3873
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42774**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3874
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42775**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3875
Loop with Unreachable Exit Condition ('Infinite Loop')	13-Dec-2022	5.5	In setEnabledSetting of PackageManager.java, there is a possible way to get the device into an infinite reboot loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-240936919 **CVE ID : CVE-2022-20476**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Dec-2022	5.5	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39106**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3877
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42779**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3878
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42780**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3879
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42781**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3880
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In audio driver, there is a use after free due to a race condition. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39134**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42770**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3882
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42771**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3883
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-Dec-2022	4.4	In writeApplicationRestrictionsLAr of UserManagerService.java , there is a possible overwrite of system files due to a path traversal error. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239701237 **CVE ID : CVE-2022-20449**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	4.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42768**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3885
Improper Authentication	08-Dec-2022	4.3	Improper authentication vulnerability in Samsung WindowManagerService prior to SMR Dec-2022 Release 1 allows attacker to send the input event using S Pen gesture. **CVE ID : CVE-2022-39899**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3886
N/A	08-Dec-2022	3.3	Improper access control vulnerabilities in Contacts prior to SMR Dec-2022 Release 1 allows to access sensitive information via implicit intent. **CVE ID : CVE-2022-39896**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3887
Integer Overflow or Wraparound	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42767**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3888
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42769**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Dec-2022	3.3	Improper access control vulnerability in IIccPhoneBook prior to SMR Dec-2022 Release 1 allows attackers to access some information of usim. **CVE ID : CVE-2022-39898**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3890
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42757**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3891
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42758**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3892
Incorrect Authorization	08-Dec-2022	3.3	Improper access control vulnerability in RCS call prior to SMR Dec-2022 Release 1 allows local attackers to access RCS incoming call number. **CVE ID : CVE-2022-39903**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3893
Exposure of Sensitive Information to an Unauthorized Actor	08-Dec-2022	3.3	Exposure of Sensitive Information vulnerability in Samsung Settings prior to SMR Dec-2022 Release 1 allows local attackers to access the Network Access Identifier via log. **CVE ID : CVE-2022-39904**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Dec-2022	3.3	Improper access control vulnerability in ContactListStartActivityHelper in Phone prior to SMR Dec-2022 Release 1 allows to access sensitive information via implicit intent. **CVE ID : CVE-2022-39894**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3895
N/A	08-Dec-2022	3.3	Improper access control vulnerability in SecTelephonyProvider prior to SMR Dec-2022 Release 1 allows attackers to access message information. **CVE ID : CVE-2022-39906**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3896
N/A	08-Dec-2022	3.3	Improper access control vulnerability in ContactListUtils in Phone prior to SMR Dec-2022 Release 1 allows to access contact group information via implicit intent. **CVE ID : CVE-2022-39895**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3897
Affected Version(s): 11.0					
Out-of-bounds Read	13-Dec-2022	9.8	In toLanguageTag of LocaleListCache.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239267173 **CVE ID : CVE-2022-20473**		
Out-of-bounds Read	13-Dec-2022	9.8	In toLanguageTag of LocaleListCache.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239210579 **CVE ID : CVE-2022-20472**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3899
Out-of-bounds Write	13-Dec-2022	8.8	In avdt_msg_asmbl of avdt_msg.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-232023771	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20411		
Out-of-bounds Write	13-Dec-2022	8.8	In avct_lcb_msg_asmbl of avct_lcb_act.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230867224 **CVE ID : CVE-2022-20469**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3901
Improper Restriction of Rendered UI Layers or Frames	13-Dec-2022	8.4	In several functions of inputDispatcher.cpp, there is a possible way to make toasts clickable due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-197296414 **CVE ID : CVE-2022-20444**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3902
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This	https://www.unisoc.com/en_us/secy/an	O-GOO-ANDR-201222/3903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39096**	nouncementDetail/15995880609884110 06	
Integer Overflow or Wraparound	08-Dec-2022	7.8	Integer overflow vulnerability in Samsung decoding library for video thumbnails prior to SMR Dec-2022 Release 1 allows local attacker to perform Out-Of-Bounds Write. **CVE ID : CVE-2022-39907**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3904
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39100**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3905
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39098**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3906
Improper Input Validation	13-Dec-2022	7.8	In bindRemoteViewsService of AppWidgetServiceImpl.ja	https://source.android.com/security/bull	O-GOO-ANDR-201222/3907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			va, there is a possible way to bypass background activity launch 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-10 Android-11 Android-12 Android-12L Android-13Android ID: A-234013191 **CVE ID : CVE-2022-20470**	etin/2022-12-01	
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39101**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3908
N/A	13-Dec-2022	7.8	In readLazyValue of Parcel.java, there is a possible loading of arbitrary code into the System Settings app due to a confused deputy. 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/2022-12-01	O-GOO-ANDR-201222/3909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-240138294 **CVE ID : CVE-2022-20474**		
N/A	13-Dec-2022	7.8	In test of ResetTargetTaskHelper.java, there is a possible hijacking of any app which sets allowTaskReparenting=" true" due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-240663194 **CVE ID : CVE-2022-20475**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3910
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39102**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3911
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-241764135 **CVE ID : CVE-2022-20478**		
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-241764340 **CVE ID : CVE-2022-20479**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3913
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-241764350 **CVE ID : CVE-2022-20480**		
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39099**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3915
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242702851 **CVE ID : CVE-2022-20484**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3916
Uncontrolled Resource	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions	https://source.android.com/security/bull	O-GOO-ANDR-201222/3917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242702935 **CVE ID : CVE-2022-20485**	etin/2022-12-01	
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242703118 **CVE ID : CVE-2022-20486**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3918
Missing Authorization	06-Dec-2022	7.8	In UscAIEngine service, there is a missing permission check. This could lead to set up UscAIEngine service with no additional execution privileges needed.	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42776		
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-42777**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3920
Missing Authorization	06-Dec-2022	7.8	In windows manager service, there is a missing permission check. This could lead to set up windows manager service with no additional execution privileges needed. **CVE ID : CVE-2022-42778**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3921
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39097**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3922
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed.	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39090		
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39091**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3924
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39092**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3925
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39093**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3926
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed.	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39094		
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39095**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3928
Integer Overflow or Wraparound	13-Dec-2022	7.5	In several functions that parse avrc response in avrc_pars_ct.cc and related files, there are possible out of bounds reads due to integer overflows. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242459126 **CVE ID : CVE-2022-20483**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3929
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Dec-2022	7.4	TOCTOU vulnerability in Samsung decoding library for video thumbnails prior to SMR Dec-2022 Release 1 allows local attacker to perform Out-Of-Bounds Write.	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39908		
Improper Restriction of Rendered UI Layers or Frames	13-Dec-2022	7.3	In onCreate of ReviewPermissionsActivity.java, there is a possible way to grant permissions for a separate app with API level < 23 due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-176094367 **CVE ID : CVE-2022-20442**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3931
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/3932
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-	O-GOO-ANDR-201222/3933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	bulletin/December-2022	
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/3934
Out-of-bounds Write	05-Dec-2022	6.7	In gz, there is a possible memory corruption 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. Patch ID: ALPS07363786; Issue ID: ALPS07363786. **CVE ID : CVE-2022-32622**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/3935
Out-of-bounds Write	05-Dec-2022	6.7	In throttling, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local	https://corp.mediatek.com/product-security-	O-GOO-ANDR-201222/3936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405923; Issue ID: ALPS07405923. **CVE ID : CVE-2022-32624**	bulletin/December-2022	
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/3937
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/3938
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, there is a possible out of bounds write due to improper input validation. This could lead to local	https://corp.mediatek.com/product-security-	O-GOO-ANDR-201222/3939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	bulletin/December-2022	
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/3940
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/3941
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of	https://corp.mediatek.com/product-security-	O-GOO-ANDR-201222/3942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	bulletin/December-2022	
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/3943
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/3944
Out-of-bounds Write	05-Dec-2022	6.7	In mpu, there is a possible memory corruption due to a logic error. This could lead to local escalation of	https://corp.mediatek.com/product-security-	O-GOO-ANDR-201222/3945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07541753; Issue ID: ALPS07541753. **CVE ID : CVE-2022-32620**	bulletin/December-2022	
Out-of-bounds Read	13-Dec-2022	6.5	In BNEP_ConnectResp of bnep_api.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-228450451 **CVE ID : CVE-2022-20468**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3946
Out-of-bounds Write	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39129**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3947
Out-of-bounds Read	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://www.unisoc.com/en_us/secy/announcementDetail/159958	O-GOO-ANDR-201222/3948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service in kernel. **CVE ID : CVE-2022-39130**	8060988411006	
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39131**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3949
Out-of-bounds Write	06-Dec-2022	5.5	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39132**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3950
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-39133**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3951
Insertion of Sensitive Information into Log File	08-Dec-2022	5.5	Exposure of Sensitive Information vulnerability in kernel prior to SMR Dec-2022 Release 1 allows attackers to access the kernel address information via log. **CVE ID : CVE-2022-39897**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3952
N/A	08-Dec-2022	5.5	Implicit intent hijacking vulnerability in Telecom application prior to SMR Dec-2022 Release 1 allows attacker to access	https://security.samsungmobile.com/securityUpdate.smsb?year=20	O-GOO-ANDR-201222/3953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive information via implicit intent. **CVE ID : CVE-2022-39905**	22&month=12	
Insecure Default Initialization of Resource	13-Dec-2022	5.5	In applyKeyguardFlags of NotificationShadeWindowControllerImpl.java, there is a possible way to observe the user's password on a secondary display due to an insecure default value. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-179725730 **CVE ID : CVE-2022-20466**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3954
N/A	08-Dec-2022	5.5	Improper access control vulnerability in Calendar prior to versions 11.6.08.0 in Android Q(10), 12.2.11.3000 in Android R(11), 12.3.07.2000 in Android S(12), and 12.4.02.0 in Android T(13) allows attackers to access sensitive information via implicit intent. **CVE ID : CVE-2022-39915**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=12	O-GOO-ANDR-201222/3955
Use After Free	06-Dec-2022	5.5	In npu driver, there is a memory corruption due	https://www.unisoc.com/e	O-GOO-ANDR-201222/3956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a use after free. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42754**	n_us/secy/announcementDetail/15995880609884110 06	
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42755**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3957
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In sensor driver, there is a possible buffer overflow due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42756**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3958
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42782**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3959
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42759**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3960
Buffer Copy without Checking Size of Input	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	O-GOO-ANDR-201222/3961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID : CVE-2022-42760**	806098841106	
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42761**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3962
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42762**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3963
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42763**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3964
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42764**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3965
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42765**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3966
Exposure of	06-Dec-2022	5.5	In wlan driver, there is a possible missing	https://www.unisoc.com/e	O-GOO-ANDR-201222/3967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42766**	n_us/secy/announcementDetail/15995880609884110 06	
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42772**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3968
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42773**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3969
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42774**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3970
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42775**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3971
Out-of-bounds Read	13-Dec-2022	5.5	In SendIncDecRestoreCmdPart2 of NxpMfcReader.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3972

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-11 Android-12 Android-12L Android-13Android ID: A-238177877 **CVE ID : CVE-2022-20471**		
Loop with Unreachable Exit Condition ('Infinite Loop')	13-Dec-2022	5.5	In setEnabledSetting of PackageManager.java, there is a possible way to get the device into an infinite reboot loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-240936919 **CVE ID : CVE-2022-20476**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3973
Out-of-bounds Write	06-Dec-2022	5.5	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39106**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42779**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3975
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42780**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3976
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42781**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3977
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In audio driver, there is a use after free due to a race condition. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39134**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3978
Concurrent Execution using Shared Resource with Improper Synchronization	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42770**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42771**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3980
N/A	08-Dec-2022	4.6	Improper access control vulnerability in Nice Catch prior to SMR Dec-2022 Release 1 allows physical attackers to access contents of all toast generated in the application installed in Secure Folder through Nice Catch. **CVE ID : CVE-2022-39900**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3981
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-Dec-2022	4.4	In writeApplicationRestrictionsLAr of UserManagerService.java, there is a possible overwrite of system files due to a path traversal error. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-239701237 **CVE ID : CVE-2022-20449**		
Out-of-bounds Read	06-Dec-2022	4.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42768**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3983
Improper Authentication	08-Dec-2022	4.3	Improper authentication vulnerability in Samsung WindowManagerService prior to SMR Dec-2022 Release 1 allows attacker to send the input event using S Pen gesture. **CVE ID : CVE-2022-39899**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3984
N/A	08-Dec-2022	3.3	Improper access control vulnerabilities in Contacts prior to SMR Dec-2022 Release 1 allows to access sensitive information via implicit intent. **CVE ID : CVE-2022-39896**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3985
Integer Overflow or Wraparound	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42767**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/3986
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to	https://www.unisoc.com/en_us/secy/announcementDetail/159958	O-GOO-ANDR-201222/3987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local denial of service in wlan services. **CVE ID : CVE-2022-42769**	8060988411006	
N/A	08-Dec-2022	3.3	Improper access control vulnerability in IIccPhoneBook prior to SMR Dec-2022 Release 1 allows attackers to access some information of usim. **CVE ID : CVE-2022-39898**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3988
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42757**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110006	O-GOO-ANDR-201222/3989
Incorrect Authorization	08-Dec-2022	3.3	Improper access control vulnerability in RCS call prior to SMR Dec-2022 Release 1 allows local attackers to access RCS incoming call number. **CVE ID : CVE-2022-39903**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3990
Exposure of Sensitive Information to an Unauthorized Actor	08-Dec-2022	3.3	Exposure of Sensitive Information vulnerability in Samsung Settings prior to SMR Dec-2022 Release 1 allows local attackers to access the Network Access Identifier via log. **CVE ID : CVE-2022-39904**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3991
N/A	08-Dec-2022	3.3	Improper access control vulnerability in ContactListStartActivityH	https://security.samsungmobile.com/sec	O-GOO-ANDR-201222/3992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			elper in Phone prior to SMR Dec-2022 Release 1 allows to access sensitive information via implicit intent. **CVE ID : CVE-2022-39894**	urityUpdate.smsb?year=2022&month=12	
N/A	08-Dec-2022	3.3	Improper access control vulnerability in SecTelephonyProvider prior to SMR Dec-2022 Release 1 allows attackers to access message information. **CVE ID : CVE-2022-39906**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3993
N/A	08-Dec-2022	3.3	Improper access control vulnerability in ContactListUtils in Phone prior to SMR Dec-2022 Release 1 allows to access contact group information via implicit intent. **CVE ID : CVE-2022-39895**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/3994
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42758**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/3995
Affected Version(s): * Up to (excluding) 13.0					
Improper Handling of Exceptional Conditions	08-Dec-2022	3.3	Improper handling of insufficient permissions vulnerability in setSecureFolderPolicy in PersonaManagerService prior to Android T(13) allows local attackers to	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=12	O-GOO-ANDR-201222/3996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			set some setting value in Secure folder. **CVE ID : CVE-2022-39912**		
Incorrect Authorization	08-Dec-2022	3.3	Exposure of Sensitive Information to an Unauthorized Actor in Persona Manager prior to Android T(13) allows local attacker to access user profiles information. **CVE ID : CVE-2022-39913**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=12	O-GOO-ANDR-201222/3997
Incorrect Authorization	08-Dec-2022	3.3	Exposure of Sensitive Information from an Unauthorized Actor vulnerability in Samsung DisplayManagerService prior to Android T(13) allows local attacker to access connected DLNA device information. **CVE ID : CVE-2022-39914**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=12	O-GOO-ANDR-201222/3998
Affected Version(s): 12.0					
Out-of-bounds Read	13-Dec-2022	9.8	In toLanguageTag of LocaleListCache.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239210579	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/3999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20472		
Out-of-bounds Read	13-Dec-2022	9.8	In toLanguageTag of LocaleListCache.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239267173 **CVE ID : CVE-2022-20473**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4000
Out-of-bounds Write	13-Dec-2022	8.8	In avdt_msg_asmbl of avdt_msg.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-232023771 **CVE ID : CVE-2022-20411**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4001
Out-of-bounds Write	13-Dec-2022	8.8	In avct_lcb_msg_asmbl of avct_lcb_act.cc, there is a possible out of bounds	https://source.android.com/security/bull	O-GOO-ANDR-201222/4002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write due to a missing bounds check. This could lead to local escalation of privilege over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230867224 **CVE ID : CVE-2022-20469**	etin/2022-12-01	
Improper Restriction of Rendered UI Layers or Frames	13-Dec-2022	8.4	In several functions of inputDispatcher.cpp, there is a possible way to make toasts clickable due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-197296414 **CVE ID : CVE-2022-20444**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4003
Improper Input Validation	13-Dec-2022	7.8	In bindRemoteViewsService of AppWidgetServiceImpl.java, there is a possible way to bypass background activity launch due to improper input validation. This	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-234013191 **CVE ID : CVE-2022-20470**		
N/A	13-Dec-2022	7.8	In readLazyValue of Parcel.java, there is a possible loading of arbitrary code into the System Settings app due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-240138294 **CVE ID : CVE-2022-20474**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4005
N/A	13-Dec-2022	7.8	In test of ResetTargetTaskHelper.java, there is a possible hijacking of any app which sets allowTaskReparenting=" true" due to a confused deputy. This could lead to local escalation of	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-240663194 **CVE ID : CVE-2022-20475**		
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-241764135 **CVE ID : CVE-2022-20478**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4007
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. 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/2022-12-01	O-GOO-ANDR-201222/4008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-241764340 **CVE ID : CVE-2022-20479**		
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-241764350 **CVE ID : CVE-2022-20480**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4009
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-242702851 **CVE ID : CVE-2022-20484**		
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242702935 **CVE ID : CVE-2022-20485**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4011
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242703118 **CVE ID : CVE-2022-20486**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39090**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4013
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39091**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4014
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39092**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4015
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39093**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39094**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4017
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39095**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4018
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39096**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4019
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39097**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39098**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4021
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39099**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4022
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39100**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4023
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39101**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-39102**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4025
Integer Overflow or Wraparound	08-Dec-2022	7.8	Integer overflow vulnerability in Samsung decoding library for video thumbnails prior to SMR Dec-2022 Release 1 allows local attacker to perform Out-Of-Bounds Write. **CVE ID : CVE-2022-39907**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4026
Missing Authorization	06-Dec-2022	7.8	In UscAIEngine service, there is a missing permission check. This could lead to set up UscAIEngine service with no additional execution privileges needed. **CVE ID : CVE-2022-42776**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4027
Missing Authorization	06-Dec-2022	7.8	In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed. **CVE ID : CVE-2022-42777**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4028
Integer Overflow	13-Dec-2022	7.5	In several functions that parse avrc response in	https://source.android.com	O-GOO-ANDR-201222/4029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			avrc_pars_ct.cc and related files, there are possible out of bounds reads due to integer overflows. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242459126 **CVE ID : CVE-2022-20483**	/security/bulletin/2022-12-01	
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Dec-2022	7.4	TOCTOU vulnerability in Samsung decoding library for video thumbnails prior to SMR Dec-2022 Release 1 allows local attacker to perform Out-Of-Bounds Write. **CVE ID : CVE-2022-39908**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4030
Improper Restriction of Rendered UI Layers or Frames	13-Dec-2022	7.3	In onCreate of ReviewPermissionsActivity.java, there is a possible way to grant permissions for a separate app with API level < 23 due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product:	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-176094367 **CVE ID : CVE-2022-20442**		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446207; Issue ID: ALPS07446207. **CVE ID : CVE-2022-32594**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4032
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446213; Issue ID: ALPS07446213. **CVE ID : CVE-2022-32596**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4033
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32597**		
Out-of-bounds Write	05-Dec-2022	6.7	In widevine, 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. Patch ID: ALPS07446228; Issue ID: ALPS07446228. **CVE ID : CVE-2022-32598**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4035
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, 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. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4036
Out-of-bounds Write	05-Dec-2022	6.7	In mpu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07541753; Issue ID: ALPS07541753. **CVE ID : CVE-2022-32620**		
Out-of-bounds Write	05-Dec-2022	6.7	In gz, there is a possible memory corruption 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. Patch ID: ALPS07363786; Issue ID: ALPS07363786. **CVE ID : CVE-2022-32622**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4038
Out-of-bounds Write	05-Dec-2022	6.7	In throttling, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405923; Issue ID: ALPS07405923. **CVE ID : CVE-2022-32624**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4039
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07326216; Issue ID: ALPS07326216. **CVE ID : CVE-2022-32625**		
Out-of-bounds Write	05-Dec-2022	6.7	In display, 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. Patch ID: ALPS07326239; Issue ID: ALPS07326239. **CVE ID : CVE-2022-32626**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4041
Out-of-bounds Write	05-Dec-2022	6.7	In isp, 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. Patch ID: ALPS07310780; Issue ID: ALPS07310780. **CVE ID : CVE-2022-32628**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4042
Out-of-bounds Write	05-Dec-2022	6.7	In isp, 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	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Patch ID: ALPS07310774; Issue ID: ALPS07310774. **CVE ID : CVE-2022-32629**		
Out-of-bounds Write	05-Dec-2022	6.7	In throttling, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405966; Issue ID: ALPS07405966. **CVE ID : CVE-2022-32630**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4044
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4045
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**		
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4047
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4048
Out-of-bounds Read	13-Dec-2022	6.5	In BNEP_ConnectResp of bnep_api.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure over	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-228450451 **CVE ID : CVE-2022-20468**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	05-Dec-2022	6.4	In isp, there is a possible out of bounds write 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. Patch ID: ALPS07310829; Issue ID: ALPS07310829. **CVE ID : CVE-2022-32621**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4050
Insecure Default Initialization of Resource	13-Dec-2022	5.5	In applyKeyguardFlags of NotificationShadeWindowControllerImpl.java, there is a possible way to observe the user's password on a secondary display due to an insecure default value. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-179725730 **CVE ID : CVE-2022-20466**		
Out-of-bounds Read	13-Dec-2022	5.5	In SendIncDecRestoreCmdPart2 of NxpMfcReader.cc, 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-11 Android-12 Android-12L Android-13Android ID: A-238177877 **CVE ID : CVE-2022-20471**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4052
Loop with Unreachable Exit Condition ('Infinite Loop')	13-Dec-2022	5.5	In setEnabledSetting of PackageManager.java, there is a possible way to get the device into an infinite reboot loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-240936919	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20476		
Uncontrolled Resource Consumption	13-Dec-2022	5.5	In createNotificationChannel of NotificationManager.java, there is a possible way to make the device unusable and require factory reset due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-240422263 **CVE ID : CVE-2022-20482**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4054
Out-of-bounds Write	06-Dec-2022	5.5	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39106**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4055
Out-of-bounds Write	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39129**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Dec-2022	5.5	In face detect driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39130**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/4057
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39131**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/4058
Out-of-bounds Write	06-Dec-2022	5.5	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39132**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/4059
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-39133**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/4060
Insertion of Sensitive Information into Log File	08-Dec-2022	5.5	Exposure of Sensitive Information vulnerability in kernel prior to SMR Dec-2022 Release 1 allows attackers to access the kernel address information via log. **CVE ID : CVE-2022-39897**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Dec-2022	5.5	Implicit intent hijacking vulnerability in Telecom application prior to SMR Dec-2022 Release 1 allows attacker to access sensitive information via implicit intent. **CVE ID : CVE-2022-39905**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4062
N/A	08-Dec-2022	5.5	Improper access control vulnerability in Calendar prior to versions 11.6.08.0 in Android Q(10), 12.2.11.3000 in Android R(11), 12.3.07.2000 in Android S(12), and 12.4.02.0 in Android T(13) allows attackers to access sensitive information via implicit intent. **CVE ID : CVE-2022-39915**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=12	O-GOO-ANDR-201222/4063
Use After Free	06-Dec-2022	5.5	In npu driver, there is a memory corruption due to a use after free. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42754**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4064
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42755**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4065
Buffer Copy without Checking	06-Dec-2022	5.5	In sensor driver, there is a possible buffer overflow due to a missing bounds check.	https://www.unisoc.com/en_us/secy/announcementD	O-GOO-ANDR-201222/4066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42756**	etail/159958806098841106	
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42759**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/4067
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42760**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/4068
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42761**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/4069
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42762**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/4070
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	O-GOO-ANDR-201222/4071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42763	8060988411006	
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42764**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/4072
Integer Overflow or Wraparound	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42765**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/4073
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42766**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/4074
Out-of-bounds Write	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42772**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/4075
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42773**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/4076
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to	https://www.unisoc.com/en_us/secy/an	O-GOO-ANDR-201222/4077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local denial of service in wlan services. **CVE ID : CVE-2022-42774**	nouncementDetail/15995880609884110 06	
Improper Locking	06-Dec-2022	5.5	In camera driver, there is a possible memory corruption due to improper locking. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-42775**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/4078
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42779**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/4079
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42780**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/4080
Out-of-bounds Read	06-Dec-2022	5.5	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42781**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/4081
Exposure of Resource to Wrong Sphere	06-Dec-2022	5.5	In wlan driver, there is a possible missing permission check, This could lead to local information disclosure. **CVE ID : CVE-2022-42782**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110 06	O-GOO-ANDR-201222/4082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In audio driver, there is a use after free due to a race condition. This could lead to local denial of service in kernel. **CVE ID : CVE-2022-39134**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4083
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42770**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4084
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Dec-2022	4.7	In wlan driver, there is a race condition, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42771**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4085
N/A	08-Dec-2022	4.6	Improper access control vulnerability in Nice Catch prior to SMR Dec-2022 Release 1 allows physical attackers to access contents of all toast generated in the application installed in Secure Folder through Nice Catch.	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39900		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-Dec-2022	4.4	In writeApplicationRestrictionsLAr of UserManagerService.java , there is a possible overwrite of system files due to a path traversal error. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239701237 **CVE ID : CVE-2022-20449**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4087
Improper Authentication	08-Dec-2022	4.3	Improper authentication vulnerability in Samsung WindowManagerService prior to SMR Dec-2022 Release 1 allows attacker to send the input event using S Pen gesture. **CVE ID : CVE-2022-39899**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4088
Out-of-bounds Read	06-Dec-2022	4.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42768**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4089
N/A	08-Dec-2022	3.3	Improper access control vulnerability in ContactListStartActivityHelper in Phone prior to	https://security.samsungmobile.com/securityUpdate.s	O-GOO-ANDR-201222/4090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMR Dec-2022 Release 1 allows to access sensitive information via implicit intent. **CVE ID : CVE-2022-39894**	msb?year=2022&month=12	
N/A	08-Dec-2022	3.3	Improper access control vulnerability in ContactListUtils in Phone prior to SMR Dec-2022 Release 1 allows to access contact group information via implicit intent. **CVE ID : CVE-2022-39895**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4091
N/A	08-Dec-2022	3.3	Improper access control vulnerabilities in Contacts prior to SMR Dec-2022 Release 1 allows to access sensitive information via implicit intent. **CVE ID : CVE-2022-39896**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4092
N/A	08-Dec-2022	3.3	Improper access control vulnerability in IIccPhoneBook prior to SMR Dec-2022 Release 1 allows attackers to access some information of usim. **CVE ID : CVE-2022-39898**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4093
Incorrect Authorization	08-Dec-2022	3.3	Improper access control vulnerability in RCS call prior to SMR Dec-2022 Release 1 allows local attackers to access RCS incoming call number.	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39903		
Exposure of Sensitive Information to an Unauthorized Actor	08-Dec-2022	3.3	Exposure of Sensitive Information vulnerability in Samsung Settings prior to SMR Dec-2022 Release 1 allows local attackers to access the Network Access Identifier via log. **CVE ID : CVE-2022-39904**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4095
N/A	08-Dec-2022	3.3	Improper access control vulnerability in SecTelephonyProvider prior to SMR Dec-2022 Release 1 allows attackers to access message information. **CVE ID : CVE-2022-39906**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4096
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42757**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4097
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42758**	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	O-GOO-ANDR-201222/4098
Integer Overflow or Wraparound	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	https://www.unisoc.com/en_us/secy/announcementDetail/159958	O-GOO-ANDR-201222/4099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42767	8060988411006	
Out-of-bounds Read	06-Dec-2022	3.3	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services. **CVE ID : CVE-2022-42769**	https://www.unisoc.com/en_us/secy/announcementDetail/15995880609884110006	O-GOO-ANDR-201222/4100
Incorrect Default Permissions	13-Dec-2022	2.3	In sOpAllowSystemRestrictionBypass of AppOpsManager.java, there is a possible leak of location information 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-12 Android-12LAndroid ID: A-231496105 **CVE ID : CVE-2022-20240**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4101
Affected Version(s): 12.1					
Out-of-bounds Read	13-Dec-2022	9.8	In toLanguageTag of LocaleListCache.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239210579 **CVE ID : CVE-2022-20472**		
Out-of-bounds Read	13-Dec-2022	9.8	In toLanguageTag of LocaleListCache.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239267173 **CVE ID : CVE-2022-20473**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4103
Out-of-bounds Write	13-Dec-2022	8.8	In avdt_msg_asmbl of avdt_msg.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-232023771	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20411		
Out-of-bounds Write	13-Dec-2022	8.8	In avct_lcb_msg_asmbl of avct_lcb_act.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230867224 **CVE ID : CVE-2022-20469**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4105
N/A	13-Dec-2022	7.8	In readLazyValue of Parcel.java, there is a possible loading of arbitrary code into the System Settings app due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-240138294 **CVE ID : CVE-2022-20474**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Dec-2022	7.8	In test of ResetTargetTaskHelper.java, there is a possible hijacking of any app which sets allowTaskReparenting=" true" due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-240663194 **CVE ID : CVE-2022-20475**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4107
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-241764135 **CVE ID : CVE-2022-20478**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4108
Uncontrolled Resource	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure	https://source.android.com/security/bull	O-GOO-ANDR-201222/4109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-241764340 **CVE ID : CVE-2022-20479**	etin/2022-12-01	
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-241764350 **CVE ID : CVE-2022-20480**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4110
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242702851 **CVE ID : CVE-2022-20484**		
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242702935 **CVE ID : CVE-2022-20485**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4112
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. 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/2022-12-01	O-GOO-ANDR-201222/4113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242703118 **CVE ID : CVE-2022-20486**		
Integer Overflow or Wraparound	13-Dec-2022	7.5	In several functions that parse avrc response in avrc_pars_ct.cc and related files, there are possible out of bounds reads due to integer overflows. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242459126 **CVE ID : CVE-2022-20483**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4114
Out-of-bounds Read	13-Dec-2022	5.5	In SendIncDecRestoreCmdPart2 of NxpMfcReader.cc, 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-11 Android-12 Android-12L Android-	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13Android ID: A-238177877 **CVE ID : CVE-2022-20471**		
Loop with Unreachable Exit Condition ('Infinite Loop')	13-Dec-2022	5.5	In setEnabledSetting of PackageManager.java, there is a possible way to get the device into an infinite reboot loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-240936919 **CVE ID : CVE-2022-20476**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4116
Uncontrolled Resource Consumption	13-Dec-2022	5.5	In createNotificationChannel of NotificationManager.java, there is a possible way to make the device unusable and require factory reset due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-240422263	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20482		
Affected Version(s): 13.0					
Out-of-bounds Read	13-Dec-2022	9.8	In toLanguageTag of LocaleListCache.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239210579 **CVE ID : CVE-2022-20472**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4118
Out-of-bounds Read	13-Dec-2022	9.8	In toLanguageTag of LocaleListCache.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239267173 **CVE ID : CVE-2022-20473**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4119
Out-of-bounds Write	13-Dec-2022	8.8	In avdt_msg_asmbl of avdt_msg.cc, there is a possible out of bounds	https://source.android.com/security/bull	O-GOO-ANDR-201222/4120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write due to a missing bounds check. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-232023771 **CVE ID : CVE-2022-20411**	etin/2022-12-01	
Out-of-bounds Write	13-Dec-2022	8.8	In avct_lcb_msg_asmbl of avct_lcb_act.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230867224 **CVE ID : CVE-2022-20469**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4121
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242703118 **CVE ID : CVE-2022-20486**		
Integer Overflow or Wraparound	08-Dec-2022	7.8	Integer overflow vulnerability in Samsung decoding library for video thumbnails prior to SMR Dec-2022 Release 1 allows local attacker to perform Out-Of-Bounds Write. **CVE ID : CVE-2022-39907**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4123
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242702851 **CVE ID : CVE-2022-20484**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	13-Dec-2022	7.8	In bindRemoteViewsService of AppWidgetServiceImpl.java, there is a possible way to bypass background activity launch 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-10 Android-11 Android-12 Android-12L Android-13Android ID: A-234013191 **CVE ID : CVE-2022-20470**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4125
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242702935 **CVE ID : CVE-2022-20485**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Dec-2022	7.8	In readLazyValue of Parcel.java, there is a possible loading of arbitrary code into the System Settings app due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-240138294 **CVE ID : CVE-2022-20474**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4127
N/A	13-Dec-2022	7.8	In test of ResetTargetTaskHelper.java, there is a possible hijacking of any app which sets allowTaskReparenting=" true" due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-240663194 **CVE ID : CVE-2022-20475**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Dec-2022	7.8	In shouldHideNotification of KeyguardNotificationVisibilityProvider.kt, there is a possible way to show hidden notifications due to a logic error in the code. 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-241611867 **CVE ID : CVE-2022-20477**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4129
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-241764135 **CVE ID : CVE-2022-20478**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4130
Uncontrolled Resource	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions	https://source.android.com/security/bull	O-GOO-ANDR-201222/4131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-241764340 **CVE ID : CVE-2022-20479**	etin/2022-12-01	
Uncontrolled Resource Consumption	13-Dec-2022	7.8	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-241764350 **CVE ID : CVE-2022-20480**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4132
Integer Overflow or Wraparound	13-Dec-2022	7.5	In several functions that parse avrc response in avrc_pars_ct.cc and related files, there are possible out of bounds reads due to integer overflows. This could lead to remote information disclosure	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4133

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-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242459126 **CVE ID : CVE-2022-20483**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Dec-2022	7.4	TOCTOU vulnerability in Samsung decoding library for video thumbnails prior to SMR Dec-2022 Release 1 allows local attacker to perform Out-Of-Bounds Write. **CVE ID : CVE-2022-39908**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4134
Out-of-bounds Write	05-Dec-2022	6.7	In mpu, there is a possible memory corruption due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07541753; Issue ID: ALPS07541753. **CVE ID : CVE-2022-32620**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4135
Out-of-bounds Write	05-Dec-2022	6.7	In gz, there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363786; Issue ID: ALPS07363786. **CVE ID : CVE-2022-32622**		
Out-of-bounds Write	05-Dec-2022	6.7	In throttling, there is a possible out of bounds write due to an incorrect calculation of buffer size. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405966; Issue ID: ALPS07405966. **CVE ID : CVE-2022-32630**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4137
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4138
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**		
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4140
Improper Input Validation	05-Dec-2022	6.7	In ccci, 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. Patch ID: ALPS07138646; Issue ID: ALPS07138646. **CVE ID : CVE-2022-32634**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4141
Out-of-bounds Write	05-Dec-2022	6.7	In keyinstall, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System	https://corp.mediatek.com/product-security-bulletin/December-2022	O-GOO-ANDR-201222/4142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07439659; Issue ID: ALPS07439659. **CVE ID : CVE-2022-32619**		
Out-of-bounds Read	13-Dec-2022	6.5	In BNEP_ConnectResp of bnep_api.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-228450451 **CVE ID : CVE-2022-20468**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4143
Insecure Default Initialization of Resource	13-Dec-2022	5.5	In applyKeyguardFlags of NotificationShadeWindowControllerImpl.java, there is a possible way to observe the user's password on a secondary display due to an insecure default value. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-179725730 **CVE ID : CVE-2022-20466**		
Out-of-bounds Read	13-Dec-2022	5.5	In SendIncDecRestoreCmdPart2 of NxpMfcReader.cc, 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-11 Android-12 Android-12L Android-13Android ID: A-238177877 **CVE ID : CVE-2022-20471**	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4145
Uncontrolled Resource Consumption	13-Dec-2022	5.5	In createNotificationChannel of NotificationManager.java, there is a possible way to make the device unusable and require factory reset due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L	https://source.android.com/security/bulletin/2022-12-01	O-GOO-ANDR-201222/4146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-240422263 **CVE ID : CVE-2022-20482**		
N/A	08-Dec-2022	5.5	Implicit intent hijacking vulnerability in Telecom application prior to SMR Dec-2022 Release 1 allows attacker to access sensitive information via implicit intent. **CVE ID : CVE-2022-39905**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4147
N/A	08-Dec-2022	5.5	Improper access control vulnerability in Calendar prior to versions 11.6.08.0 in Android Q(10), 12.2.11.3000 in Android R(11), 12.3.07.2000 in Android S(12), and 12.4.02.0 in Android T(13) allows attackers to access sensitive information via implicit intent. **CVE ID : CVE-2022-39915**	https://security.samsungmobile.com/serviceWeb.smsb?year=2022&month=12	O-GOO-ANDR-201222/4148
N/A	08-Dec-2022	4.6	Improper access control vulnerability in Nice Catch prior to SMR Dec-2022 Release 1 allows physical attackers to access contents of all toast generated in the application installed in Secure Folder through Nice Catch. **CVE ID : CVE-2022-39900**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4149
Improper Limitation	13-Dec-2022	4.4	In writeApplicationRestricti	https://source.android.com	O-GOO-ANDR-201222/4150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			onsLAr of UserManagerService.java , there is a possible overwrite of system files due to a path traversal error. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239701237 **CVE ID : CVE-2022-20449**	/security/bulletin/2022-12-01	
Improper Authentication	08-Dec-2022	4.3	Improper authentication vulnerability in Samsung WindowManagerService prior to SMR Dec-2022 Release 1 allows attacker to send the input event using S Pen gesture. **CVE ID : CVE-2022-39899**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4151
N/A	08-Dec-2022	3.3	Improper access control vulnerability in IIccPhoneBook prior to SMR Dec-2022 Release 1 allows attackers to access some information of usim. **CVE ID : CVE-2022-39898**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4152
Incorrect Authorization	08-Dec-2022	3.3	Improper access control vulnerability in RCS call prior to SMR Dec-2022 Release 1 allows local attackers to access RCS incoming call number.	https://security.samsungmobile.com/securityUpdate.smsb?year=20	O-GOO-ANDR-201222/4153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39903	22&month=12	
N/A	08-Dec-2022	3.3	Improper access control vulnerability in SecTelephonyProvider prior to SMR Dec-2022 Release 1 allows attackers to access message information. **CVE ID : CVE-2022-39906**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-GOO-ANDR-201222/4154
Vendor: hornerautomation					
Product: rcc972_firmware					
Affected Version(s): 15.40					
Use of Hard-coded Cryptographic Key	02-Dec-2022	9.8	Horner Automation's RCC 972 with firmware version 15.40 has a static encryption key on the device. This could allow an attacker to perform unauthorized changes to the device, remotely execute arbitrary code, or cause a denial-of-service condition. **CVE ID : CVE-2022-2641**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-335-02	O-HOR-RCC9-201222/4155
Inadequate Encryption Strength	02-Dec-2022	7.5	The Config-files of Horner Automation's RCC 972 with firmware version 15.40 are encrypted with weak XOR encryption vulnerable to reverse engineering. This could allow an attacker to obtain credentials to run services such as File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP).	https://www.cisa.gov/uscert/ics/advisories/icsa-22-335-02	O-HOR-RCC9-201222/4156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2640		
Excessive Reliance on Global Variables	02-Dec-2022	7.5	Horner Automation's RCC 972 firmware version 15.40 contains global variables. This could allow an attacker to read out sensitive values and variable keys from the device. **CVE ID : CVE-2022-2642**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-335-02	O-HOR-RCC9-201222/4157
Vendor: HP					
Product: m2u75a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U7-201222/4158
Product: m2u76a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U7-201222/4159
Product: m2u77a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack.	https://support.hp.com/us-en/document/ish_7095452-7095489-	O-HP-M2U7-201222/4160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43780	16/hpsbpi03813	
Product: m2u81a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U8-201222/4161
Product: m2u81b_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U8-201222/4162
Product: m2u82a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U8-201222/4163
Product: m2u82b_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U8-201222/4164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: m2u84a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U8-201222/4165
Product: m2u84b_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U8-201222/4166
Product: m2u85a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U8-201222/4167
Product: m2u85b_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U8-201222/4168
Product: m2u86a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U8-201222/4169
Product: m2u86b_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U8-201222/4170
Product: m2u86c_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U8-201222/4171
Product: m2u87a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U8-201222/4172
Product: m2u87b_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet	https://support.hp.com/us-	O-HP-M2U8-201222/4173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	en/document/ish_7095452-7095489-16/hpsbpi03813	
Product: m2u88b_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U8-201222/4174
Product: m2u89b_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U8-201222/4175
Product: m2u91a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U9-201222/4176
Product: m2u91b_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be	https://support.hp.com/us-en/document/ish_7095452	O-HP-M2U9-201222/4177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	-7095489-16/hpsbpi03813	
Product: m2u92a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U9-201222/4178
Product: m2u92b_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U9-201222/4179
Product: m2u94a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-M2U9-201222/4180
Product: m2u94b_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack.	https://support.hp.com/us-en/document/ish_7095452-7095489-	O-HP-M2U9-201222/4181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43780	16/hpsbpi03813	
Product: pagewide_352dw_j6u57a_firmware					
Affected Version(s): * Up to (excluding) 2228b					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	O-HP-PAGE-201222/4182
Product: pagewide_377dw_j9v80a_firmware					
Affected Version(s): * Up to (excluding) 2228b					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	O-HP-PAGE-201222/4183
Product: pagewide_managed_p55250dw_j6u51b_firmware					
Affected Version(s): * Up to (excluding) 2228b					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	O-HP-PAGE-201222/4184
Product: pagewide_managed_p55250dw_j6u55a_firmware					
Affected Version(s): * Up to (excluding) 2228b					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	O-HP-PAGE-201222/4185
Product: pagewide_managed_p55250dw_j6u55b_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2228b					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	O-HP-PAGE-201222/4186
Product: pagewide_managed_p57750dw_j9v82a_firmware					
Affected Version(s): * Up to (excluding) 2228b					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	O-HP-PAGE-201222/4187
Product: pagewide_pro_452dn_d3q15a_firmware					
Affected Version(s): * Up to (excluding) 2228b					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	O-HP-PAGE-201222/4188
Product: pagewide_pro_452dw_d3q16a_firmware					
Affected Version(s): * Up to (excluding) 2228b					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	O-HP-PAGE-201222/4189
Product: pagewide_pro_477dn_d3q19a_firmware					
Affected Version(s): * Up to (excluding) 2228b					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be	https://support.hp.com/us-	O-HP-PAGE-201222/4190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	en/document/ish_6720386-6720411-16/hpsbpi03807	
Product: pagewide_pro_477dw_d3q20a_firmware					
Affected Version(s): * Up to (excluding) 2228b					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	O-HP-PAGE-201222/4191
Product: pagewide_pro_552dw_d3q17a_firmware					
Affected Version(s): * Up to (excluding) 2228b					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	O-HP-PAGE-201222/4192
Product: pagewide_pro_577dw_d3q21a_firmware					
Affected Version(s): * Up to (excluding) 2228b					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack. **CVE ID : CVE-2022-2794**	https://support.hp.com/us-en/document/ish_6720386-6720411-16/hpsbpi03807	O-HP-PAGE-201222/4193
Product: pagewide_pro_577z_k9z76a_firmware					
Affected Version(s): * Up to (excluding) 2228b					
N/A	12-Dec-2022	7.5	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack.	https://support.hp.com/us-en/document/ish_6720386-6720411-	O-HP-PAGE-201222/4194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2794	16/hpsbpi03807	
Product: z4a54a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-Z4A5-201222/4195
Product: z4a59a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-Z4A5-201222/4196
Product: z4a60a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-Z4A6-201222/4197
Product: z4a61a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-Z4A6-201222/4198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: z4a61b_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-Z4A6-201222/4199
Product: z4a69a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-Z4A6-201222/4200
Product: z4a70a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-Z4A7-201222/4201
Product: z4a71a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-Z4A7-201222/4202
Product: z4a73a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-Z4A7-201222/4203
Product: z4a74a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-Z4A7-201222/4204
Product: z4b12a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-Z4B1-201222/4205
Product: z4b13a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-Z4B1-201222/4206
Product: z4b14a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet	https://support.hp.com/us-	O-HP-Z4B1-201222/4207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	en/document/ish_7095452-7095489-16/hpsbpi03813	
Product: z4b18a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-Z4B1-201222/4208
Product: z4b27a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-Z4B2-201222/4209
Product: z4b28a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	https://support.hp.com/us-en/document/ish_7095452-7095489-16/hpsbpi03813	O-HP-Z4B2-201222/4210
Product: z4b29a_firmware					
Affected Version(s): * Up to (excluding) 003.2237a					
N/A	12-Dec-2022	7.5	Certain HP ENVY, OfficeJet, and DeskJet printers may be	https://support.hp.com/us-en/document/ish_7095452	O-HP-Z4B2-201222/4211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to a Denial of Service attack. **CVE ID : CVE-2022-43780**	-7095489-16/hpsbpi03813	
Vendor: hpe					
Product: hf20c_firmware					
Affected Version(s): * Up to (excluding) 5.2.1.900					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	O-HPE-HF20-201222/4212
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	O-HPE-HF20-201222/4213
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	O-HPE-HF20-201222/4214
Affected Version(s): 5.3.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	O-HPE-HF20-201222/4215
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	O-HPE-HF20-201222/4216
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	O-HPE-HF20-201222/4217
Product: hf20h_firmware					
Affected Version(s): * Up to (excluding) 5.2.1.900					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	O-HPE-HF20-201222/4218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37928	hpesbst04359en_us	
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	O-HPE-HF20-201222/4219
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	O-HPE-HF20-201222/4220
Affected Version(s): 5.3.0.0					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	O-HPE-HF20-201222/4221
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	O-HPE-HF20-201222/4222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	hpesbst04360en_us	
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	O-HPE-HF20-201222/4223
Product: hf20_firmware					
Affected Version(s): * Up to (excluding) 5.2.1.900					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	O-HPE-HF20-201222/4224
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	O-HPE-HF20-201222/4225
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and	https://support.hpe.com/hpsc/doc/public/display?docL	O-HPE-HF20-201222/4226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	ocale=en_US&docId=emr_na-hpesbst04361en_us	
Affected Version(s): 5.3.0.0					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	O-HPE-HF20-201222/4227
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	O-HPE-HF20-201222/4228
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	O-HPE-HF20-201222/4229
Product: hf40c_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 5.2.1.900					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	O-HPE-HF40-201222/4230
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	O-HPE-HF40-201222/4231
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	O-HPE-HF40-201222/4232
Affected Version(s): 5.3.0.0					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	O-HPE-HF40-201222/4233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37928	hpesbst04359en_us	
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	O-HPE-HF40-201222/4234
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	O-HPE-HF40-201222/4235
Product: hf40_firmware					
Affected Version(s): * Up to (excluding) 5.2.1.900					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	O-HPE-HF40-201222/4236
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na	O-HPE-HF40-201222/4237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	-hpesbst04360en_us	
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	O-HPE-HF40-201222/4238
Affected Version(s): 5.3.0.0					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	O-HPE-HF40-201222/4239
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	O-HPE-HF40-201222/4240
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&	O-HPE-HF40-201222/4241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	docId=emr_na-hpesbst04361en_us	
Product: hf60c_firmware					
Affected Version(s): * Up to (excluding) 5.2.1.900					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	O-HPE-HF60-201222/4242
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	O-HPE-HF60-201222/4243
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	O-HPE-HF60-201222/4244
Affected Version(s): 5.3.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	O-HPE-HF60-201222/4245
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	O-HPE-HF60-201222/4246
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	O-HPE-HF60-201222/4247
Product: hf60_firmware					
Affected Version(s): * Up to (excluding) 5.2.1.900					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	O-HPE-HF60-201222/4248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37928	hpesbst04359en_us	
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	O-HPE-HF60-201222/4249
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	O-HPE-HF60-201222/4250
Affected Version(s): 5.3.0.0					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	O-HPE-HF60-201222/4251
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	O-HPE-HF60-201222/4252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	hpesbst04360en_us	
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	O-HPE-HF60-201222/4253
Product: sf100_firmware					
Affected Version(s): * Up to (excluding) 5.2.1.900					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	O-HPE-SF10-201222/4254
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	O-HPE-SF10-201222/4255
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and	https://support.hpe.com/hpsc/doc/public/display?docL	O-HPE-SF10-201222/4256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	ocale=en_US&docId=emr_na-hpesbst04361en_us	
Affected Version(s): 5.3.0.0					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	O-HPE-SF10-201222/4257
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	O-HPE-SF10-201222/4258
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	O-HPE-SF10-201222/4259
Product: sf300_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 5.2.1.900					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37928**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04359en_us	O-HPE-SF30-201222/4260
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	O-HPE-SF30-201222/4261
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	O-HPE-SF30-201222/4262
Affected Version(s): 5.3.0.0					
Insufficient Verification of Data Authenticity	12-Dec-2022	6.5	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	O-HPE-SF30-201222/4263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37928	hpesbst04359en_us	
Improper Privilege Management	12-Dec-2022	5.5	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays. **CVE ID : CVE-2022-37929**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04360en_us	O-HPE-SF30-201222/4264
N/A	12-Dec-2022	5.5	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information. **CVE ID : CVE-2022-37930**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst04361en_us	O-HPE-SF30-201222/4265
Vendor: IBM					
Product: aix					
Affected Version(s): -					
Use of a Broken or Risky Cryptographic Algorithm	06-Dec-2022	7.5	IBM Sterling Secure Proxy 6.0.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 230522. **CVE ID : CVE-2022-34361**	https://www.ibm.com/support/pages/node/6844763	O-IBM-AIX-201222/4266
Product: linux_on_zseries					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of a Broken or Risky Cryptographic Algorithm	06-Dec-2022	7.5	IBM Sterling Secure Proxy 6.0.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 230522. **CVE ID : CVE-2022-34361**	https://www.ibm.com/support/pages/node/6844763	O-IBM-LINU-201222/4267
Product: power_system_ac922_\(8335-gtg\)_firmware					
Affected Version(s): From (including) op910 Up to (including) op910.70					
Allocation of Resources Without Limits or Throttling	12-Dec-2022	4.9	IBM OpenBMC OP910 and OP940 could allow a privileged user to cause a denial of service by uploading or deleting too many CA certificates in a short period of time. IBM X-Force ID: 2226337. **CVE ID : CVE-2022-22488**	https://exchange.xforce.ibmcloud.com/vulnerabilities/226337, https://www.ibm.com/support/pages/node/6840155	O-IBM-POWE-201222/4268
Product: power_system_ac922_\(8335-gth\)_firmware					
Affected Version(s): From (including) op940 Up to (including) op940.40					
Allocation of Resources Without Limits or Throttling	12-Dec-2022	4.9	IBM OpenBMC OP910 and OP940 could allow a privileged user to cause a denial of service by uploading or deleting too many CA certificates in a short period of time. IBM X-Force ID: 2226337. **CVE ID : CVE-2022-22488**	https://exchange.xforce.ibmcloud.com/vulnerabilities/226337, https://www.ibm.com/support/pages/node/6840155	O-IBM-POWE-201222/4269
Product: power_system_ac922_\(8335-gtx\)_firmware					
Affected Version(s): From (including) op940 Up to (including) op940.40					
Allocation of Resources	12-Dec-2022	4.9	IBM OpenBMC OP910 and OP940 could allow a privileged user to cause a	https://exchange.xforce.ibmcloud.com/v	O-IBM-POWE-201222/4270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Without Limits or Throttling			denial of service by uploading or deleting too many CA certificates in a short period of time. IBM X-Force ID: 2226337. **CVE ID : CVE-2022-22488**	ulnerabilities/226337, https://www.ibm.com/support/pages/node/6840155	
Vendor: ifm					
Product: moneo_qha200_firmware					
Affected Version(s): * Up to (including) 1.9.3					
Weak Password Recovery Mechanism for Forgotten Password	12-Dec-2022	7.5	In IFM Moneo Appliance with version up to 1.9.3 an unauthenticated remote attacker can reset the administrator password by only supplying the serial number. **CVE ID : CVE-2022-3485**	N/A	O-IFM-MONE-201222/4271
Product: moneo_qha210_firmware					
Affected Version(s): * Up to (including) 1.9.3					
Weak Password Recovery Mechanism for Forgotten Password	12-Dec-2022	7.5	In IFM Moneo Appliance with version up to 1.9.3 an unauthenticated remote attacker can reset the administrator password by only supplying the serial number. **CVE ID : CVE-2022-3485**	N/A	O-IFM-MONE-201222/4272
Vendor: Kyocera					
Product: ecosys_m2535dn_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document	https://www.kyoceradocumentsolutions.co.jp/support	O-KYO-ECOS-201222/4273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent	https://www.kyoceradocumentsolutions.co.jp/support/information/info_2022110	O-KYO-ECOS-201222/4274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	1.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46	O-KYO-ECOS-201222/4275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	345126/index.html	
Product: ecosys_m6526cdn_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-ECOS-201222/4276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-ECOS-201222/4277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-ECOS-201222/4278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: ecosys_m6526cidn_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-ECOS-201222/4279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-ECOS-201222/4280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-ECOS-201222/4281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: ecosys_p2135dn_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-ECOS-201222/4282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-ECOS-201222/4283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100 DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-ECOS-201222/4284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: ecosys_p4040dn_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-ECOS-201222/4285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN.	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-ECOS-201222/4286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41807		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-ECOS-201222/4287
Product: ecosys_p6026cdn_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-ECOS-201222/4288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-ECOS-201222/4289
Improper Neutralization of	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document	https://www.kyoceradocumentsolutions	O-KYO-ECOS-201222/4290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Product: fs-1370dn_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may	https://www.kyoceradocumentsolutions.co.jp/support/information/info_2022110	O-KYO-FS-1-201222/4291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	1.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp	O-KYO-FS-1-201222/4292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	/en/jp/JVN46345126/index.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-FS-1-201222/4293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: fs-c2026mfp_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-FS-C-201222/4294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-FS-C-201222/4295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-FS-C-201222/4296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: fs-c2126mfp\+_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-FS-C-201222/4297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-FS-C-201222/4298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-FS-C-201222/4299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: fs-c2126mfp_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-FS-C-201222/4300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-FS-C-201222/4301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-FS-C-201222/4302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: fs-c5250dn_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-FS-C-201222/4303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN.	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-FS-C-201222/4304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41807		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-FS-C-201222/4305
Product: ls-1035mfp_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-1-201222/4306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-1-201222/4307
Improper Neutralization of	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document	https://www.kyoceradocumentsolutions	O-KYO-LS-1-201222/4308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Product: ls-1135mfp_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may	https://www.kyoceradocumentsolutions.co.jp/support/information/info_2022110	O-KYO-LS-1-201222/4309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	1.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp	O-KYO-LS-1-201222/4310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	/en/jp/JVN46345126/index.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-1-201222/4311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: ls-2100dn_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-2-201222/4312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-2-201222/4313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-2-201222/4314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: ls-3140mfp\+_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-3-201222/4315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-3-201222/4316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-3-201222/4317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: ls-3140mfp_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-3-201222/4318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-3-201222/4319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-3-201222/4320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: ls-3640mfp_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-3-201222/4321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN.	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-3-201222/4322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41807		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-3-201222/4323
Product: ls-4200dn_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-4-201222/4324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-4-201222/4325
Improper Neutralization of	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document	https://www.kyoceradocumentsolutions	O-KYO-LS-4-201222/4326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Product: ls-4300dn_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may	https://www.kyoceradocumentsolutions.co.jp/support/information/info_2022110	O-KYO-LS-4-201222/4327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	1.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp	O-KYO-LS-4-201222/4328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	/en/jp/JVN46345126/index.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-4-201222/4329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: ls-c8600dn_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-C-201222/4330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-C-201222/4331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-C-201222/4332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: ls-c8650dn_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-C-201222/4333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-C-201222/4334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-LS-C-201222/4335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_205c_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_206ci_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN.	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41807		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4341
Product: taskalfa_255c_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4343
Improper Neutralization of	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document	https://www.kyoceradocumentsolutions	O-KYO-TASK-201222/4344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Product: taskalfa_255_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may	https://www.kyoceradocumentsolutions.co.jp/support/information/info_2022110	O-KYO-TASK-201222/4345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	1.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp	O-KYO-TASK-201222/4346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	/en/jp/JVN46345126/index.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_256ci_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_256i_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_3050ci_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_305_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN.	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41807		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4359
Product: taskalfa_306i_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4361
Improper Neutralization of	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document	https://www.kyoceradocumentsolutions	O-KYO-TASK-201222/4362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Product: taskalfa_3500i_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may	https://www.kyoceradocumentsolutions.co.jp/support/information/info_2022110	O-KYO-TASK-201222/4363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	1.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp	O-KYO-TASK-201222/4364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	/en/jp/JVN46345126/index.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_3550ci_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_4500i_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_4550ci_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_5500i_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN.	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41807		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4377
Product: taskalfa_5550ci_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4379
Improper Neutralization of	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document	https://www.kyoceradocumentsolutions	O-KYO-TASK-201222/4380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**	.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Product: taskalfa_6500i_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may	https://www.kyoceradocumentsolutions.co.jp/support/information/info_2022110	O-KYO-TASK-201222/4381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**	1.html, https://jvn.jp/en/jp/JVN46345126/index.html	
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp	O-KYO-TASK-201222/4382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**	/en/jp/JVN46345126/index.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_6550ci_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_7550ci_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Product: taskalfa_8000i_firmware					
Affected Version(s): -					
Authentication Bypass by Spoofing	05-Dec-2022	6.5	Session information easily guessable vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to log in to the product by spoofing a user with guessed session information. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41798**		
Missing Authorization	05-Dec-2022	6.5	Missing authorization vulnerability exists in Kyocera Document Solutions MFPs and printers, which may allow a network-adjacent attacker to alter the product settings without authentication by sending a specially crafted request. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn, ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41807**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Dec-2022	4.8	Stored cross-site scripting vulnerability in Kyocera Document Solutions MFPs and printers allows a remote authenticated attacker with an administrative privilege to inject arbitrary script. Affected products/versions are as follows: TASKalfa 7550ci/6550ci, TASKalfa 5550ci/4550ci/3550ci/3050ci, TASKalfa 255c/205c, TASKalfa 256ci/206ci, ECOSYS M6526cdn/M6526cidn, FS-C2126MFP/C2126MFP+/C2026MFP/C2026MFP+, TASKalfa 8000i/6500i, TASKalfa 5500i/4500i/3500i, TASKalfa 305/255, TASKalfa 306i/256i, LS-3140MFP/3140MFP+/3640MFP, ECOSYS M2535dn, LS-1135MFP/1035MFP, LS-C8650DN/C8600DN, ECOSYS P6026cdn, FS-C5250DN, LS-4300DN/4200DN/2100DN, ECOSYS P4040dn,	https://www.kyoceradocumentsolutions.co.jp/support/information/info_20221101.html, https://jvn.jp/en/jp/JVN46345126/index.html	O-KYO-TASK-201222/4392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ECOSYS P2135dn, and FS-1370DN. **CVE ID : CVE-2022-41830**		
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Dec-2022	7.8	IBM Spectrum Scale 5.1.0.1 through 5.1.4.1 could allow a local attacker to execute arbitrary commands in the container. IBM X-Force ID: 239437. **CVE ID : CVE-2022-43867**	https://www.ibm.com/support/pages/node/6844771	O-LIN-LINU-201222/4393
Use of a Broken or Risky Cryptographic Algorithm	06-Dec-2022	7.5	IBM Sterling Secure Proxy 6.0.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 230522. **CVE ID : CVE-2022-34361**	https://www.ibm.com/support/pages/node/6844763	O-LIN-LINU-201222/4394
Insufficiently Protected Credentials	09-Dec-2022	5.5	Insufficiently Protected Credentials vulnerability in the remote backups application on Western Digital My Cloud devices that could allow an attacker who has gained access to a relevant endpoint to use that information to access protected data. This issue affects: Western	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	O-LIN-LINU-201222/4395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29839**		
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	O-LIN-LINU-201222/4396
Affected Version(s): * Up to (excluding) 6.0					
Improper Locking	07-Dec-2022	5.5	Guests can trigger deadlock in Linux netback driver T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] The patch for XSA-392 introduced another issue which might result in a deadlock when trying to free the SKB of a packet dropped due to the XSA-392 handling (CVE-2022-42328). Additionally when dropping packages for other reasons the same deadlock could occur in	http://www.openwall.com/lists/oss-security/2022/12/08/3, http://www.openwall.com/lists/oss-security/2022/12/08/2, http://www.openwall.com/lists/oss-security/2022/12/09/2	O-LIN-LINU-201222/4397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			case of netpoll being active for the interface the xen-netback driver is connected to (CVE-2022-42329). **CVE ID : CVE-2022-42328**		
Improper Locking	07-Dec-2022	5.5	Guests can trigger deadlock in Linux netback driver T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] The patch for XSA-392 introduced another issue which might result in a deadlock when trying to free the SKB of a packet dropped due to the XSA-392 handling (CVE-2022-42328). Additionally when dropping packages for other reasons the same deadlock could occur in case of netpoll being active for the interface the xen-netback driver is connected to (CVE-2022-42329). **CVE ID : CVE-2022-42329**	https://xenbits.xenproject.org/xsa/advisory-424.txt, http://www.openwall.com/lists/oss-security/2022/12/08/3, http://www.openwall.com/lists/oss-security/2022/12/08/2, http://www.openwall.com/lists/oss-security/2022/12/09/2	O-LIN-LINU-201222/4398
Affected Version(s): 4.1					
Deadlock	05-Dec-2022	5.5	A flaw was found in the Linux kernel Traffic Control (TC) subsystem. Using a specific networking configuration (redirecting egress	https://lore.kernel.org/netdev/33dc43f587ec1388ba456b4915c75f02a8aae226.1663945716.gi	O-LIN-LINU-201222/4399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packets to ingress using TC action "mirred") a local unprivileged user could trigger a CPU soft lockup (ABBA deadlock) when the transport protocol in use (TCP or SCTP) does a retransmission, resulting in a denial of service condition. **CVE ID : CVE-2022-4269**	t.dcaratti@redhat.com/	
Affected Version(s): From (including) 3.19 Up to (excluding) 4.14					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	07-Dec-2022	10	Guests can trigger NIC interface reset/abort/crash via netback It is possible for a guest to trigger a NIC interface reset/abort/crash in a Linux based network backend by sending certain kinds of packets. It appears to be an (unwritten?) assumption in the rest of the Linux network stack that packet protocol headers are all contained within the linear section of the SKB and some NICs behave badly if this is not the case. This has been reported to occur with Cisco (enic) and Broadcom NetXtrem II BCM5780 (bnx2x) though it may be an issue with other NICs/drivers as well. In case the frontend is sending requests with split	https://xenbits.xenproject.org/xsa/advisory-423.txt	O-LIN-LINU-201222/4400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			headers, netback will forward those violating above mentioned assumption to the networking core, resulting in said misbehavior. **CVE ID : CVE-2022-3643**		
Vendor: Medtronic					
Product: guardian_link_2_transmitter_mmt-7730_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-GUAR-201222/4401
Product: guardian_link_2_transmitter_mmt-7731_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol	https://global.medtronic.com/xg-en/product-security/secu	O-MED-GUAR-201222/4402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	rity-bulletins/minimed-600-series-communication-issue.html	
Product: guardian_link_2_transmitter_mmt-7738_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-GUAR-201222/4403
Product: guardian_link_2_transmitter_mmt-7775_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-GUAR-201222/4404
Product: guardian_link_3_transmitter_mmt-7810_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-GUAR-201222/4405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**		
Product: guardian_link_3_transmitter_mmt-7811_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-GUAR-201222/4406
Product: minimed_620g_mmt-1750_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components.	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-	O-MED-MINI-201222/4407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	communication-issue.html	
Product: minimed_630g_mmt-1715_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-MINI-201222/4408
Product: minimed_630g_mmt-1754_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to	https://global.medtronic.com/xg-	O-MED-MINI-201222/4409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	en/product-security/security-bulletins/minimed-600-series-communication-issue.html	
Product: minimed_630g_mmt-1755_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-MINI-201222/4410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32537		
Product: minimed_640g_mmt-1711_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-MINI-201222/4411
Product: minimed_640g_mmt-1712_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device;	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-MINI-201222/4412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**		
Product: minimed_640g_mmt-1751_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-MINI-201222/4413
Product: minimed_640g_mmt-1752_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the	https://global.medtronic.com/xg-en/product-security/security-bulletins/mini	O-MED-MINI-201222/4414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	med-600-series-communication-issue.html	
Product: minimed_670g_mmt-1740_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-MINI-201222/4415
Product: minimed_670g_mmt-1741_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-MINI-201222/4416
Product: minimed_670g_mmt-1742_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-MINI-201222/4417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**		
Product: minimed_670g_mmt-1760_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-MINI-201222/4418
Product: minimed_670g_mmt-1761_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-MINI-201222/4419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**		
Product: minimed_670g_mmt-1762_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-MINI-201222/4420
Product: minimed_670g_mmt-1780_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the	https://global.medtronic.com/xg-en/product-	O-MED-MINI-201222/4421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	security/security-bulletins/minimed-600-series-communication-issue.html	
Product: minimed_670g_mmt-1781_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-MINI-201222/4422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: minimed_670g_mmt-1782_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-MINI-201222/4423
Product: mmt-1151_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-MMT--201222/4424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**		
Product: mmt-1152_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-MMT-201222/4425
Product: mmt-1351_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-	O-MED-MMT-201222/4426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	communication-issue.html	
Product: mmt-1352_firmware					
Affected Version(s): -					
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-MMT--201222/4427
Product: mmt-7306_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2022	4.8	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance **CVE ID : CVE-2022-32537**	https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html	O-MED-MMT--201222/4428
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Out-of-bounds Write	12-Dec-2022	7.8	An out-of-bounds access vulnerability in the Unauthorized Change Prevention service of Trend Micro Apex One and Apex One as a Service could allow a local attacker to elevate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	https://success.trendmicro.com/solution/000291770	O-MIC-WIND-201222/4429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-44649		
Out-of-bounds Write	12-Dec-2022	7.8	A memory corruption vulnerability in the Unauthorized Change Prevention service of Trend Micro Apex One and Apex One as a Service could allow a local attacker to elevate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-44650**	https://success.trendmicro.com/solution/000291770	O-MIC-WIND-201222/4430
Use of a Broken or Risky Cryptographic Algorithm	06-Dec-2022	7.5	IBM Sterling Secure Proxy 6.0.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 230522. **CVE ID : CVE-2022-34361**	https://www.ibm.com/support/pages/node/6844763	O-MIC-WIND-201222/4431
Improper Neutralization of Special Elements in Output Used by a Downstream Component	09-Dec-2022	7.5	Crash in the USB HID protocol dissector in Wireshark 3.6.0 to 3.6.8 allows denial of service via packet injection or crafted capture file on Windows **CVE ID : CVE-2022-3724**	https://www.wireshark.org/security/wnpa-sec-2022-08.html, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-	O-MIC-WIND-201222/4432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')				2022-3724.json	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Dec-2022	7.5	On Windows, restricted files can be accessed via os.DirFS and http.Dir. The os.DirFS function and http.Dir type provide access to a tree of files rooted at a given directory. These functions permit access to Windows device files under that root. For example, os.DirFS("C:/tmp").Open("COM1") opens the COM1 device. Both os.DirFS and http.Dir only provide read-only filesystem access. In addition, on Windows, an os.DirFS for the directory (the root of the current drive) can permit a maliciously crafted path to escape from the drive and access any path on the system. With fix applied, the behavior of os.DirFS("") has changed. Previously, an empty root was treated equivalently to "/", so os.DirFS("").Open("tmp") would open the path "/tmp". This now returns an error. **CVE ID : CVE-2022-41720**	https://groups.google.com/g/golang-announce/c/L_3rmdT0BMU/m/yZDrXjIiBQAJ, https://pkg.go.dev/vuln/GO-2022-1143, https://go.dev/cl/455716, https://go.dev/issue/56694	O-MIC-WIND-201222/4433
N/A	12-Dec-2022	7.1	An arbitrary file deletion vulnerability in the Damage Cleanup Engine component of Trend	https://success.trendmicro.com/solution/000291830	O-MIC-WIND-201222/4434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Micro Apex One and Trend Micro Apex One as a Service could allow a local attacker to escalate privileges and delete files on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-45797**		
Improper Handling of Insufficient Privileges	12-Dec-2022	6.8	A privilege escalation issue exists within the Amazon CloudWatch Agent for Windows, software for collecting metrics and logs from Amazon EC2 instances and on-premises servers, in versions up to and including v1.247354. When users trigger a repair of the Agent, a pop-up window opens with SYSTEM permissions. Users with administrative access to affected hosts may use this to create a new command prompt as NT AUTHORITY\SYSTEM. To trigger this issue, the third party must be able to access the affected host and elevate their privileges such that they're able to trigger the agent repair process. They must also be able to install the tools required	https://github.com/aws/amazon-cloudwatch-agent/security/advisories/GHSA-j8x2-2m5w-j939, https://github.com/aws/amazon-cloudwatch-agent/commit/6119858864c317ff26f41f576c169148d1250837#diff-76ed074a9305c04054cdebb9e9aad2d818052b07091de1f20cad0bbac34ffb52	O-MIC-WIND-201222/4435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to trigger the issue. This issue does not affect the CloudWatch Agent for macOS or Linux. Agent users should upgrade to version 1.247355 of the CloudWatch Agent to address this issue. There is no recommended work around. Affected users must update the installed version of the CloudWatch Agent to address this issue. **CVE ID : CVE-2022-23511**		
Out-of-bounds Read	12-Dec-2022	5.5	An Out-of-bounds read vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to disclose sensitive information on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is similar to, but not the same as CVE-2022-44648. **CVE ID : CVE-2022-44647**	https://success.trendmicro.com/solution/000291770	O-MIC-WIND-201222/4436
Out-of-bounds Read	12-Dec-2022	5.5	An Out-of-bounds read vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to disclose sensitive information on affected installations.	https://success.trendmicro.com/solution/000291770	O-MIC-WIND-201222/4437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is similar to, but not the same as CVE-2022-44647. **CVE ID : CVE-2022-44648**		
Generation of Error Message Containing Sensitive Information	06-Dec-2022	3.3	Generation of Error Message Containing Sensitive Information vulnerability in Hitachi JP1/Automatic Operation allows local users to gain sensitive information. This issue affects JP1/Automatic Operation: from 10-00 through 10-54-03, from 11-00 before 11-51-09, from 12-00 before 12-60-01. **CVE ID : CVE-2022-34881**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2022-140/index.html	O-MIC-WIND-201222/4438
Vendor: Mikrotik					
Product: routeros					
Affected Version(s): * Up to (excluding) 7.5					
Out-of-bounds Read	05-Dec-2022	9.8	Mikrotik RouterOs before stable v7.5 was discovered to contain an out-of-bounds read in the hotspot process. This vulnerability allows attackers to execute arbitrary code via a crafted nova message. **CVE ID : CVE-2022-45313**	N/A	O-MIK-ROUT-201222/4439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 7.6					
Out-of-bounds Read	05-Dec-2022	9.8	Mikrotik RouterOs before stable v7.6 was discovered to contain an out-of-bounds read in the snmp process. This vulnerability allows attackers to execute arbitrary code via a crafted packet. **CVE ID : CVE-2022-45315**	N/A	O-MIK-ROUT-201222/4440
Vendor: Moxa					
Product: uc-2101-lx_firmware					
Affected Version(s): From (including) 1.3 Up to (including) 1.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-2-201222/4441
Product: uc-2102-lx_firmware					
Affected Version(s): From (including) 1.3 Up to (including) 1.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may	N/A	O-MOX-UC-2-201222/4442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-2104-lx_firmware					
Affected Version(s): From (including) 1.3 Up to (including) 1.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-2-201222/4443
Product: uc-2111-lx_firmware					
Affected Version(s): From (including) 1.3 Up to (including) 1.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-2-201222/4444
Product: uc-2112-lx_firmware					
Affected Version(s): From (including) 1.3 Up to (including) 1.5					
Improper Neutralization of Special	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell	N/A	O-MOX-UC-2-201222/4445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-2114-t-lx_firmware					
Affected Version(s): From (including) 1.3 Up to (including) 1.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-2-201222/4446
Product: uc-2116-t-lx_firmware					
Affected Version(s): From (including) 1.3 Up to (including) 1.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-2-201222/4447
Product: uc-3101-t-ap-lx_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-3-201222/4448
Product: uc-3101-t-eu-lx_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-3-201222/4449
Product: uc-3101-t-us-lx_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may	N/A	O-MOX-UC-3-201222/4450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-3111-t-ap-lx-nw_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-3-201222/4451
Product: uc-3111-t-ap-lx_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-3-201222/4452
Product: uc-3111-t-eu-lx-nw_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Neutralization of Special	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell	N/A	O-MOX-UC-3-201222/4453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-3111-t-eu-lx_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-3-201222/4454
Product: uc-3111-t-us-lx-nw_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-3-201222/4455
Product: uc-3111-t-us-lx_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-3-201222/4456
Product: uc-3121-t-ap-lx_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-3-201222/4457
Product: uc-3121-t-eu-lx_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may	N/A	O-MOX-UC-3-201222/4458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-3121-t-us-lx_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-3-201222/4459
Product: uc-5101-lx_firmware					
Affected Version(s): 1.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-5-201222/4460
Product: uc-5101-t-lx_firmware					
Affected Version(s): 1.2					
Improper Neutralization of Special	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell	N/A	O-MOX-UC-5-201222/4461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-5102-lx_firmware					
Affected Version(s): 1.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-5-201222/4462
Product: uc-5102-t-lx_firmware					
Affected Version(s): 1.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-5-201222/4463
Product: uc-5111-lx_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-5-201222/4464
Product: uc-5111-t-lx_firmware					
Affected Version(s): 1.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-5-201222/4465
Product: uc-5112-lx_firmware					
Affected Version(s): 1.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may	N/A	O-MOX-UC-5-201222/4466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-5112-t-lx_firmware					
Affected Version(s): 1.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-5-201222/4467
Product: uc-8112-lx_firmware					
Affected Version(s): 1.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4468
Affected Version(s): 1.3					
Improper Neutralization of Special Elements	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables	N/A	O-MOX-UC-8-201222/4469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-8112a-me-t-lx_firmware					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4470
Affected Version(s): 1.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4471
Product: uc-8131-lx_firmware					
Affected Version(s): 1.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4472
Affected Version(s): 1.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4473
Product: uc-8132-lx_firmware					
Affected Version(s): 1.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code.	N/A	O-MOX-UC-8-201222/4474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3086		
Affected Version(s): 1.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4475
Product: uc-8162-lx_firmware					
Affected Version(s): 1.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4476
Affected Version(s): 1.3					
Improper Neutralization of Special Elements used in a Command ('Comman	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may	N/A	O-MOX-UC-8-201222/4477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-8210-t-lx-s_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 2.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4478
Product: uc-8220-t-lx-ap-s_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 2.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4479
Product: uc-8220-t-lx-eu-s_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 2.4					
Improper Neutralization of Special	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell	N/A	O-MOX-UC-8-201222/4480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-8220-t-lx-us-s_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 2.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4481
Product: uc-8220-t-lx_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 2.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4482
Product: uc-8410a-lx_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4483
Product: uc-8410a-nw-lx_firmware					
Affected Version(s): 2.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4484
Product: uc-8410a-nw-t-lx_firmware					
Affected Version(s): 2.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may	N/A	O-MOX-UC-8-201222/4485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-8410a-t-lx_firmware					
Affected Version(s): 2.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4486
Product: uc-8540-lx_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 1.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4487
Product: uc-8540-t-ct-lx_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 1.2					
Improper Neutralization of Special	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell	N/A	O-MOX-UC-8-201222/4488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-8540-t-lx_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 1.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4489
Product: uc-8580-lx_firmware					
Affected Version(s): 1.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4490
Product: uc-8580-q-lx_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4491
Product: uc-8580-t-ct-lx_firmware					
Affected Version(s): 1.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4492
Product: uc-8580-t-ct-q-lx_firmware					
Affected Version(s): 1.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may	N/A	O-MOX-UC-8-201222/4493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**		
Product: uc-8580-t-lx_firmware					
Affected Version(s): 1.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4494
Product: uc-8580-t-q-lx_firmware					
Affected Version(s): 1.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-Dec-2022	7.6	Cradlepoint IBR600 NCOS versions 6.5.0.160bc2e and prior are vulnerable to shell escape, which enables local attackers with non-superuser credentials to gain full, unrestrictive shell access which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2022-3086**	N/A	O-MOX-UC-8-201222/4495
Vendor: Ricoh					
Product: aficio_sp_4210n_firmware					
Affected Version(s): * Up to (excluding) 1.05					
Improper Neutralizat	07-Dec-2022	4.8	Cross-site scripting vulnerability in Aficio SP	https://support.ricoh.com/	O-RIC-AFIC-201222/4496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			4210N firmware versions prior to Web Support 1.05 allows a remote authenticated attacker with an administrative privilege to inject an arbitrary script. **CVE ID : CVE-2022-37406**	bb/html/dr_ut_e/rc3/model/sp42/sp42.htm, https://support.ricoh.com/bbv2/html/dr_ut_d/ipsio/history/w/bb/pub_j/dr_ut_d/4101044/4101044791/V101/5236968/redirect_CLUTool_DOM/history.htm	
Vendor: Samsung					
Product: exynos_firmware					
Affected Version(s): -					
Incorrect Authorization	08-Dec-2022	7.5	Improper authorization in Exynos baseband prior to SMR DEC-2022 Release 1 allows remote attacker to get sensitive information including IMEI via emergency call. **CVE ID : CVE-2022-39902**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-SAM-EXYN-201222/4497
Improper Authentication	08-Dec-2022	6.5	Improper authentication in Exynos baseband prior to SMR DEC-2022 Release 1 allows remote attacker to disable the network traffic encryption between UE and gNodeB. **CVE ID : CVE-2022-39901**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=12	O-SAM-EXYN-201222/4498
Vendor: secu					
Product: secustation_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.3.4.1301-m20-tsa-b20150617a					
Cleartext Transmission of Sensitive Information	08-Dec-2022	4.9	In certain Secustation products the administrator account password can be read. This affects V2.5.5.3116-S50-SMA-B20171107A, V2.3.4.1301-M20-TSA-B20150617A, V2.5.5.3116-S50-RXA-B20180502A, V2.5.5.3116-S50-SMA-B20190723A, V2.5.5.3116-S50-SMB-B20161012A, V2.3.4.2103-S50-NTD-B20170508B, V2.5.5.3116-S50-SMB-B20160601A, V2.5.5.2601-S50-TSA-B20151229A, and V2.5.5.3116-S50-SMA-B20170217. **CVE ID : CVE-2022-40939**	N/A	O-SEC-SECU-201222/4499
Affected Version(s): 2.3.4.2103-s50-ntd-b20170508b					
Cleartext Transmission of Sensitive Information	08-Dec-2022	4.9	In certain Secustation products the administrator account password can be read. This affects V2.5.5.3116-S50-SMA-B20171107A, V2.3.4.1301-M20-TSA-B20150617A, V2.5.5.3116-S50-RXA-B20180502A, V2.5.5.3116-S50-SMA-B20190723A, V2.5.5.3116-S50-SMB-B20161012A, V2.3.4.2103-S50-NTD-B20170508B, V2.5.5.3116-S50-SMB-	N/A	O-SEC-SECU-201222/4500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			B20160601A, V2.5.5.2601-S50-TSA-B20151229A, and V2.5.5.3116-S50-SMA-B20170217. **CVE ID : CVE-2022-40939**		
Affected Version(s): 2.5.5.2601-s50-tsa-b20151229a					
Cleartext Transmission of Sensitive Information	08-Dec-2022	4.9	In certain Secustation products the administrator account password can be read. This affects V2.5.5.3116-S50-SMA-B20171107A, V2.3.4.1301-M20-TSA-B20150617A, V2.5.5.3116-S50-RXA-B20180502A, V2.5.5.3116-S50-SMA-B20190723A, V2.5.5.3116-S50-SMB-B20161012A, V2.3.4.2103-S50-NTD-B20170508B, V2.5.5.3116-S50-SMB-B20160601A, V2.5.5.2601-S50-TSA-B20151229A, and V2.5.5.3116-S50-SMA-B20170217. **CVE ID : CVE-2022-40939**	N/A	O-SEC-SECU-201222/4501
Affected Version(s): 2.5.5.3116-s50-rxa-b20180502a					
Cleartext Transmission of Sensitive Information	08-Dec-2022	4.9	In certain Secustation products the administrator account password can be read. This affects V2.5.5.3116-S50-SMA-B20171107A, V2.3.4.1301-M20-TSA-B20150617A, V2.5.5.3116-S50-RXA-	N/A	O-SEC-SECU-201222/4502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			B20180502A, V2.5.5.3116-S50-SMA-B20190723A, V2.5.5.3116-S50-SMB-B20161012A, V2.3.4.2103-S50-NTD-B20170508B, V2.5.5.3116-S50-SMB-B20160601A, V2.5.5.2601-S50-TSA-B20151229A, and V2.5.5.3116-S50-SMA-B20170217. **CVE ID : CVE-2022-40939**		
Affected Version(s): 2.5.5.3116-s50-sma-b20170217					
Cleartext Transmission of Sensitive Information	08-Dec-2022	4.9	In certain Secustation products the administrator account password can be read. This affects V2.5.5.3116-S50-SMA-B20171107A, V2.3.4.1301-M20-TSA-B20150617A, V2.5.5.3116-S50-RXA-B20180502A, V2.5.5.3116-S50-SMA-B20190723A, V2.5.5.3116-S50-SMB-B20161012A, V2.3.4.2103-S50-NTD-B20170508B, V2.5.5.3116-S50-SMB-B20160601A, V2.5.5.2601-S50-TSA-B20151229A, and V2.5.5.3116-S50-SMA-B20170217. **CVE ID : CVE-2022-40939**	N/A	O-SEC-SECU-201222/4503
Affected Version(s): 2.5.5.3116-s50-sma-b20171107a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	08-Dec-2022	4.9	In certain Secustation products the administrator account password can be read. This affects V2.5.5.3116-S50-SMA-B20171107A, V2.3.4.1301-M20-TSA-B20150617A, V2.5.5.3116-S50-RXA-B20180502A, V2.5.5.3116-S50-SMA-B20190723A, V2.5.5.3116-S50-SMB-B20161012A, V2.3.4.2103-S50-NTD-B20170508B, V2.5.5.3116-S50-SMB-B20160601A, V2.5.5.2601-S50-TSA-B20151229A, and V2.5.5.3116-S50-SMA-B20170217. **CVE ID : CVE-2022-40939**	N/A	O-SEC-SECU-201222/4504
Affected Version(s): 2.5.5.3116-s50-sma-b20190723a					
Cleartext Transmission of Sensitive Information	08-Dec-2022	4.9	In certain Secustation products the administrator account password can be read. This affects V2.5.5.3116-S50-SMA-B20171107A, V2.3.4.1301-M20-TSA-B20150617A, V2.5.5.3116-S50-RXA-B20180502A, V2.5.5.3116-S50-SMA-B20190723A, V2.5.5.3116-S50-SMB-B20161012A, V2.3.4.2103-S50-NTD-B20170508B, V2.5.5.3116-S50-SMB-B20160601A,	N/A	O-SEC-SECU-201222/4505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V2.5.5.2601-S50-TSA-B20151229A, and V2.5.5.3116-S50-SMA-B20170217. **CVE ID : CVE-2022-40939**		
Affected Version(s): 2.5.5.3116-s50-smb-b20160601a					
Cleartext Transmission of Sensitive Information	08-Dec-2022	4.9	In certain Secustation products the administrator account password can be read. This affects V2.5.5.3116-S50-SMA-B20171107A, V2.3.4.1301-M20-TSA-B20150617A, V2.5.5.3116-S50-RXA-B20180502A, V2.5.5.3116-S50-SMA-B20190723A, V2.5.5.3116-S50-SMB-B20161012A, V2.3.4.2103-S50-NTD-B20170508B, V2.5.5.3116-S50-SMB-B20160601A, V2.5.5.2601-S50-TSA-B20151229A, and V2.5.5.3116-S50-SMA-B20170217. **CVE ID : CVE-2022-40939**	N/A	O-SEC-SECU-201222/4506
Affected Version(s): 2.5.5.3116-s50-smb-b20161012a					
Cleartext Transmission of Sensitive Information	08-Dec-2022	4.9	In certain Secustation products the administrator account password can be read. This affects V2.5.5.3116-S50-SMA-B20171107A, V2.3.4.1301-M20-TSA-B20150617A, V2.5.5.3116-S50-RXA-B20180502A,	N/A	O-SEC-SECU-201222/4507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V2.5.5.3116-S50-SMA-B20190723A, V2.5.5.3116-S50-SMB-B20161012A, V2.3.4.2103-S50-NTD-B20170508B, V2.5.5.3116-S50-SMB-B20160601A, V2.5.5.2601-S50-TSA-B20151229A, and V2.5.5.3116-S50-SMA-B20170217. **CVE ID : CVE-2022-40939**		
Vendor: Sophos					
Product: xg_firewall_firmware					
Affected Version(s): * Up to (including) 19.0					
Improper Control of Generation of Code ('Code Injection')	01-Dec-2022	8.8	A code injection vulnerability allows adjacent attackers to execute code in the Wifi controller of Sophos Firewall releases older than version 19.5 GA. **CVE ID : CVE-2022-3713**	https://www.sophos.com/en-us/security-advisories/sophos-sa-20221201-sfos-19-5-0	O-SOP-XG_F-201222/4508
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Dec-2022	8.4	A stored XSS vulnerability allows admin to super-admin privilege escalation in the Webadmin import group wizard of Sophos Firewall releases older than version 19.5 GA. **CVE ID : CVE-2022-3709**	https://www.sophos.com/en-us/security-advisories/sophos-sa-20221201-sfos-19-5-0	O-SOP-XG_F-201222/4509
Improper Neutralization of Special Elements	01-Dec-2022	7.2	An OS command injection vulnerability allows admins to execute code via SSL VPN configuration uploads in	https://www.sophos.com/en-us/security-advisories/sophos-sa-	O-SOP-XG_F-201222/4510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Sophos Firewall releases older than version 19.5 GA. **CVE ID : CVE-2022-3226**	20221201-sfos-19-5-0	
Improper Control of Generation of Code ('Code Injection')	01-Dec-2022	7.2	A post-auth code injection vulnerability allows admins to execute code in Webadmin of Sophos Firewall releases older than version 19.5 GA. **CVE ID : CVE-2022-3696**	https://www.sophos.com/en-us/security-advisories/sophos-sa-20221201-sfos-19-5-0	O-SOP-XG_F-201222/4511
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Dec-2022	4.3	A post-auth read-only SQL injection vulnerability allows users to read non-sensitive configuration database contents in the User Portal of Sophos Firewall releases older than version 19.5 GA. **CVE ID : CVE-2022-3711**	https://www.sophos.com/en-us/security-advisories/sophos-sa-20221201-sfos-19-5-0	O-SOP-XG_F-201222/4512
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Dec-2022	2.7	A post-auth read-only SQL injection vulnerability allows API clients to read non-sensitive configuration database contents in the API controller of Sophos Firewall releases older than version 19.5 GA. **CVE ID : CVE-2022-3710**	https://www.sophos.com/en-us/security-advisories/sophos-sa-20221201-sfos-19-5-0	O-SOP-XG_F-201222/4513
Vendor: telos					
Product: omnia_mpx_node_firmware					
Affected Version(s): From (including) 1.0.0 Up to (including) 1.4.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	02-Dec-2022	8.8	Insecure permissions in Telos Alliance Omnia MPX Node v1.0.0 to v1.4.9 allow attackers to manipulate and access system settings with backdoor account low privilege, this can lead to change hardware settings and execute arbitrary commands in vulnerable system functions that is requires high privilege to access. **CVE ID : CVE-2022-45562**	N/A	O-TEL-OMNI-201222/4514
Vendor: telosalliance					
Product: omnia_mpx_node_firmware					
Affected Version(s): 1.3.35					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Dec-2022	9.8	An unauthenticated command injection vulnerability in the product license validation function of Telos Alliance Omnia MPX Node 1.3.* - 1.4.* allows attackers to execute arbitrary commands via a crafted payload injected into the license input. **CVE ID : CVE-2022-43325**	N/A	O-TEL-OMNI-201222/4515
Affected Version(s): 1.3.37					
Improper Neutralization of Special Elements used in an OS	02-Dec-2022	9.8	An unauthenticated command injection vulnerability in the product license validation function of Telos Alliance Omnia MPX Node 1.3.* - 1.4.*	N/A	O-TEL-OMNI-201222/4516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			allows attackers to execute arbitrary commands via a crafted payload injected into the license input. **CVE ID : CVE-2022-43325**		
Vendor: Tenda					
Product: a18_firmware					
Affected Version(s): 15.13.07.09					
Out-of-bounds Write	08-Dec-2022	7.5	Tenda A18 v15.13.07.09 was discovered to contain a stack overflow via the security_5g parameter at /goform/WifiBasicSet. **CVE ID : CVE-2022-44931**	https://github.com/z1r00/IOT_Vul/blob/main/Tenda/A18/formWifiBasicSet/readme.md	O-TEN-A18_-201222/4517
N/A	08-Dec-2022	7.5	An access control issue in Tenda A18 v15.13.07.09 allows unauthenticated attackers to access the Telnet service. **CVE ID : CVE-2022-44932**	N/A	O-TEN-A18_-201222/4518
Product: ac6_firmware					
Affected Version(s): 15.03.05.19					
Out-of-bounds Write	01-Dec-2022	7.5	Tenda Tenda AC6V1.0 V15.03.05.19 is affected by buffer overflow. Causes a denial of service (local). **CVE ID : CVE-2022-45640**	N/A	O-TEN-AC6_-201222/4519
Buffer Copy without Checking Size of Input	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 is vulnerable to Buffer Overflow via formSetMacFilterCfg.	N/A	O-TEN-AC6_-201222/4520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID : CVE-2022-45641**		
Cross-Site Request Forgery (CSRF)	02-Dec-2022	6.5	Tenda AC6V1.0 V15.03.05.19 is vulnerable to Cross Site Request Forgery (CSRF) via function fromSysToolRestoreSet. **CVE ID : CVE-2022-45673**	N/A	O-TEN-AC6_-201222/4521
Cross-Site Request Forgery (CSRF)	02-Dec-2022	6.5	Tenda AC6V1.0 V15.03.05.19 is vulnerable to Cross Site Request Forgery (CSRF) via function fromSysToolReboot. **CVE ID : CVE-2022-45674**	N/A	O-TEN-AC6_-201222/4522
Product: ax12_firmware					
Affected Version(s): 22.03.01.16_cn					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Dec-2022	8.8	Tenda AX12 V22.03.01.16_cn is vulnerable to command injection via goform/fast_setting_internet_set. **CVE ID : CVE-2022-45043**	N/A	O-TEN-AX12-201222/4523
Affected Version(s): 22.03.01.21_cn					
Improper Neutralization of Special Elements used in a Command ('Comman	12-Dec-2022	8.8	Tenda AX12 V22.03.01.21_CN was found to have a command injection vulnerability via /goform/setMacFilterCfg function.	N/A	O-TEN-AX12-201222/4524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			**CVE ID : CVE-2022-45977**		
Cross-Site Request Forgery (CSRF)	12-Dec-2022	8.8	Tenda AX12 V22.03.01.21_CN was discovered to contain a Cross-Site Request Forgery (CSRF) via /goform/SysToolRestoreSet . **CVE ID : CVE-2022-45980**	N/A	O-TEN-AX12-201222/4525
Out-of-bounds Write	12-Dec-2022	7.5	Tenda AX12 v22.03.01.21_CN was discovered to contain a stack overflow via the ssid parameter at /goform/fast_setting_wifi_set . **CVE ID : CVE-2022-45979**	N/A	O-TEN-AX12-201222/4526
Product: i21_firmware					
Affected Version(s): 1.0.0.14\\(4656\\)					
Out-of-bounds Write	02-Dec-2022	9.8	Tenda i21 V1.0.0.14(4656) is vulnerable to Buffer Overflow via /goform/AddSysLogRule . **CVE ID : CVE-2022-44362**	N/A	O-TEN-I21_-201222/4527
Out-of-bounds Write	02-Dec-2022	9.8	Tenda i21 V1.0.0.14(4656) is vulnerable to Buffer Overflow via /goform/setSnmpInfo. **CVE ID : CVE-2022-44363**	N/A	O-TEN-I21_-201222/4528
Out-of-bounds Write	02-Dec-2022	9.8	Tenda i21 V1.0.0.14(4656) has a stack overflow	N/A	O-TEN-I21_-201222/4529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability via /goform/setSysPwd. **CVE ID : CVE-2022-44365**		
Out-of-bounds Write	02-Dec-2022	9.8	Tenda i21 V1.0.0.14(4656) is vulnerable to Buffer Overflow via /goform/setDiagnoseInfo. **CVE ID : CVE-2022-44366**	N/A	O-TEN-I21_-201222/4530
Out-of-bounds Write	02-Dec-2022	9.8	Tenda i21 V1.0.0.14(4656) is vulnerable to Buffer Overflow via /goform/setUplinkInfo. **CVE ID : CVE-2022-44367**	N/A	O-TEN-I21_-201222/4531
Product: i22_firmware					
Affected Version(s): 1.0.0.3\\(4687\\)					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the index parameter in the formWifiMacFilterSet function. **CVE ID : CVE-2022-45663**	N/A	O-TEN-I22_-201222/4532
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the list parameter in the formwrlSSIDget function. **CVE ID : CVE-2022-45664**	N/A	O-TEN-I22_-201222/4533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the index parameter in the formWifiMacFilterGet function. **CVE ID : CVE-2022-45669**	N/A	O-TEN-I22_-201222/4534
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the ping1 parameter in the formSetAutoPing function. **CVE ID : CVE-2022-45670**	N/A	O-TEN-I22_-201222/4535
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the appData parameter in the formSetAppFilterRule function. **CVE ID : CVE-2022-45671**	N/A	O-TEN-I22_-201222/4536
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the formWx3AuthorizeSet function. **CVE ID : CVE-2022-45672**	N/A	O-TEN-I22_-201222/4537
Cross-Site Request Forgery (CSRF)	02-Dec-2022	6.5	Tenda i22 V1.0.0.3(4687) is vulnerable to Cross Site Request Forgery (CSRF)	N/A	O-TEN-I22_-201222/4538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via function fromSysToolRestoreSet. **CVE ID : CVE-2022-45667**		
Cross-Site Request Forgery (CSRF)	02-Dec-2022	6.5	Tenda i22 V1.0.0.3(4687) is vulnerable to Cross Site Request Forgery (CSRF) via function fromSysToolReboot. **CVE ID : CVE-2022-45668**	N/A	O-TEN-I22_-201222/4539
Product: w20e_firmware					
Affected Version(s): 16.01.0.6\\(3392\\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-Dec-2022	7.2	Tenda W20E V16.01.0.6(3392) is vulnerable to Command injection via cmd_get_ping_output. **CVE ID : CVE-2022-45996**	N/A	O-TEN-W20E-201222/4540
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Dec-2022	7.2	Tenda W20E V16.01.0.6(3392) is vulnerable to Buffer Overflow. **CVE ID : CVE-2022-45997**	N/A	O-TEN-W20E-201222/4541
Product: w30e_firmware					
Affected Version(s): 1.0.1.25\\(633\\)					
Improper Neutralization of Special Elements used in a	08-Dec-2022	9.8	Tenda W30E v1.0.1.25(633) was discovered to contain a command injection vulnerability via the	N/A	O-TEN-W30E-201222/4542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			fileNameMit parameter at /goform/delFileName. **CVE ID : CVE-2022-45506**		
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the cmdinput parameter at /goform/exeCommand. **CVE ID : CVE-2022-45505**	N/A	O-TEN-W30E-201222/4543
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the editNameMit parameter at /goform/editFileName. **CVE ID : CVE-2022-45507**	N/A	O-TEN-W30E-201222/4544
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the new_account parameter at /goform/editUserName. **CVE ID : CVE-2022-45508**	N/A	O-TEN-W30E-201222/4545
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the account parameter at /goform/addUserName. **CVE ID : CVE-2022-45509**	N/A	O-TEN-W30E-201222/4546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the mit_ssid_index parameter at /goform/AdvSetWrlsafeset. **CVE ID : CVE-2022-45510**	N/A	O-TEN-W30E-201222/4547
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the PPPOEPassword parameter at /goform/QuickIndex. **CVE ID : CVE-2022-45511**	N/A	O-TEN-W30E-201222/4548
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/SafeEmailFilter. **CVE ID : CVE-2022-45512**	N/A	O-TEN-W30E-201222/4549
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/P2pListFilter. **CVE ID : CVE-2022-45513**	N/A	O-TEN-W30E-201222/4550
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at	N/A	O-TEN-W30E-201222/4551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/goform/webExcptypemanFilter. **CVE ID : CVE-2022-45514**		
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the entries parameter at /goform/addressNat. **CVE ID : CVE-2022-45515**	N/A	O-TEN-W30E-201222/4552
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/NatStaticSetting. **CVE ID : CVE-2022-45516**	N/A	O-TEN-W30E-201222/4553
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/VirtualSer. **CVE ID : CVE-2022-45517**	N/A	O-TEN-W30E-201222/4554
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/SetIpBind. **CVE ID : CVE-2022-45518**	N/A	O-TEN-W30E-201222/4555
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the Go	N/A	O-TEN-W30E-201222/4556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter at /goform/SafeMacFilter. **CVE ID : CVE-2022-45519**		
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/qossetting. **CVE ID : CVE-2022-45520**	N/A	O-TEN-W30E-201222/4557
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/SafeUrlFilter. **CVE ID : CVE-2022-45521**	N/A	O-TEN-W30E-201222/4558
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/SafeClientFilter. **CVE ID : CVE-2022-45522**	N/A	O-TEN-W30E-201222/4559
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/L7Im. **CVE ID : CVE-2022-45523**	N/A	O-TEN-W30E-201222/4560
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the	N/A	O-TEN-W30E-201222/4561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			opttype parameter at /goform/IPSECsave. **CVE ID : CVE-2022-45524**		
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the downaction parameter at /goform/CertListInfo. **CVE ID : CVE-2022-45525**	N/A	O-TEN-W30E-201222/4562
Product: w6-s_firmware					
Affected Version(s): 1.0.0.4\\(510\\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Dec-2022	9.8	Tenda W6-S v1.0.0.4(510) was discovered to contain a command injection vulnerability in the tpi_get_ping_output function at /goform/exeCommand. **CVE ID : CVE-2022-45497**	N/A	O-TEN-W6-S-201222/4563
N/A	08-Dec-2022	7.5	An issue in the component tpi_systool_handle(0) (/goform/SysToolReboot) of Tenda W6-S v1.0.0.4(510) allows unauthenticated attackers to arbitrarily reboot the device. **CVE ID : CVE-2022-45498**	N/A	O-TEN-W6-S-201222/4564
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W6-S v1.0.0.4(510) was discovered to contain a stack overflow via the wl_radio parameter at	N/A	O-TEN-W6-S-201222/4565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/goform/WifiMacFilterGet. **CVE ID : CVE-2022-45499**		
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W6-S v1.0.0.4(510) was discovered to contain a stack overflow via the wl_radio parameter at /goform/wifiSSIDset. **CVE ID : CVE-2022-45501**	N/A	O-TEN-W6-S-201222/4566
Out-of-bounds Write	08-Dec-2022	7.5	Tenda W6-S v1.0.0.4(510) was discovered to contain a stack overflow via the linkEn parameter at /goform/setAutoPing. **CVE ID : CVE-2022-45503**	N/A	O-TEN-W6-S-201222/4567
N/A	08-Dec-2022	7.5	An issue in the component tpi_systool_handle(0) (/goform/SysToolRestoreSet) of Tenda W6-S v1.0.0.4(510) allows unauthenticated attackers to arbitrarily reboot the device. **CVE ID : CVE-2022-45504**	N/A	O-TEN-W6-S-201222/4568
Vendor: Tendacn					
Product: ac6_firmware					
Affected Version(s): 15.03.05.19					
Buffer Copy without Checking Size of Input	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the deviceId parameter in	N/A	O-TEN-AC6_-201222/4569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			the addWifiMacFilter function. **CVE ID : CVE-2022-45643**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the deviceId parameter in the formSetClientState function. **CVE ID : CVE-2022-45644**	N/A	O-TEN-AC6_-201222/4570
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the deviceMac parameter in the addWifiMacFilter function. **CVE ID : CVE-2022-45645**	N/A	O-TEN-AC6_-201222/4571
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the limitSpeedUp parameter in the formSetClientState function. **CVE ID : CVE-2022-45646**	N/A	O-TEN-AC6_-201222/4572
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the limitSpeed parameter in the formSetClientState function. **CVE ID : CVE-2022-45647**	N/A	O-TEN-AC6_-201222/4573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the devName parameter in the formSetDeviceName function. **CVE ID : CVE-2022-45648**	N/A	O-TEN-AC6_-201222/4574
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the endIp parameter in the formSetPPTPServer function. **CVE ID : CVE-2022-45649**	N/A	O-TEN-AC6_-201222/4575
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the firewallEn parameter in the formSetFirewallCfg function. **CVE ID : CVE-2022-45650**	N/A	O-TEN-AC6_-201222/4576
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the list parameter in the formSetVirtualSer function. **CVE ID : CVE-2022-45651**	N/A	O-TEN-AC6_-201222/4577
Buffer Copy without Checking Size of	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the startIp parameter in the	N/A	O-TEN-AC6_-201222/4578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			formSetPPTPServer function. **CVE ID : CVE-2022-45652**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the page parameter in the fromNatStaticSetting function. **CVE ID : CVE-2022-45653**	N/A	O-TEN-AC6_-201222/4579
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the ssid parameter in the form_fast_setting_wifi_set function. **CVE ID : CVE-2022-45654**	N/A	O-TEN-AC6_-201222/4580
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the timeZone parameter in the form_fast_setting_wifi_set function. **CVE ID : CVE-2022-45655**	N/A	O-TEN-AC6_-201222/4581
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the time parameter in the fromSetSysTime function. **CVE ID : CVE-2022-45656**	N/A	O-TEN-AC6_-201222/4582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the list parameter in the fromSetIpMacBind function. **CVE ID : CVE-2022-45657**	N/A	O-TEN-AC6_-201222/4583
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the schedEndTime parameter in the setSchedWifi function. **CVE ID : CVE-2022-45658**	N/A	O-TEN-AC6_-201222/4584
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the wpapsk_crypto parameter in the fromSetWirelessRepeat function. **CVE ID : CVE-2022-45659**	N/A	O-TEN-AC6_-201222/4585
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the schedStartTime parameter in the setSchedWifi function. **CVE ID : CVE-2022-45660**	N/A	O-TEN-AC6_-201222/4586
Buffer Copy without Checking	02-Dec-2022	7.5	Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the	N/A	O-TEN-AC6_-201222/4587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			time parameter in the setSmartPowerManagement function. **CVE ID : CVE-2022-45661**		
Vendor: Tp-link					
Product: re3000_firmware					
Affected Version(s): * Up to (excluding) 221009					
Improper Input Validation	07-Dec-2022	5.5	tdpServer of TP-Link RE300 V1 improperly processes its input, which may allow an attacker to cause a denial-of-service (DoS) condition of the product's OneMesh function. **CVE ID : CVE-2022-41783**	https://www.tp-link.com/en/support/download/re300/v1/#Firmware	O-TP--RE30-201222/4588
Product: tl-wr740n_firmware					
Affected Version(s): -					
Improper Resource Shutdown or Release	06-Dec-2022	5.5	A vulnerability classified as problematic has been found in TP-Link TL-WR740N. Affected is an unknown function of the component ARP Handler. The manipulation leads to resource consumption. The attack needs to be done within the local network. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-214812. **CVE ID : CVE-2022-4296**	N/A	O-TP--TL-W-201222/4589
Vendor: Trendnet					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: tew-820ap_firmware					
Affected Version(s): 1.01.b01					
Out-of-bounds Write	07-Dec-2022	8.8	A stack overflow vulnerability exists in TrendNet Wireless AC Easy-Upgrader TEW-820AP (Version v1.0R, firmware version 1.01.B01) which may result in remote code execution. **CVE ID : CVE-2022-44373**	N/A	O-TRE-TEW--201222/4590
Vendor: ui					
Product: edgemax_edgerouter_firmware					
Affected Version(s): * Up to (excluding) 2.0.9					
N/A	05-Dec-2022	8.8	A remote code execution vulnerability in EdgeRouters (Version 2.0.9-hotfix.4 and earlier) allows a malicious actor with an operator account to run arbitrary administrator commands.This vulnerability is fixed in Version 2.0.9-hotfix.5 and later. **CVE ID : CVE-2022-43553**	https://community.ui.com/releases/Security-Advisory-Bulletin-026-026/07697c65-30b3-4c06-a158-35e06534480d	O-UI-EDGE-201222/4591
Affected Version(s): 2.0.9					
N/A	05-Dec-2022	8.8	A remote code execution vulnerability in EdgeRouters (Version 2.0.9-hotfix.4 and earlier) allows a malicious actor with an operator account to run arbitrary administrator commands.This vulnerability is fixed in	https://community.ui.com/releases/Security-Advisory-Bulletin-026-026/07697c65-30b3-4c06-a158-	O-UI-EDGE-201222/4592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Version 2.0.9-hotfix.5 and later. **CVE ID : CVE-2022-43553**	35e06534480d	
Vendor: unimo					
Product: udr-ja1604_firmware					
Affected Version(s): * Up to (excluding) 71x10.1.107114.43a					
N/A	07-Dec-2022	8.8	Hidden functionality vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings. **CVE ID : CVE-2022-43464**	http://www.unimo.co.jp/table_notice/index.php?act=1&resid=1666831567-004418	O-UNI-UDR--201222/4593
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Dec-2022	8.8	OS command injection vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings. **CVE ID : CVE-2022-44606**	http://www.unimo.co.jp/table_notice/index.php?act=1&resid=1666831567-004418	O-UNI-UDR--201222/4594
Improper Authentication	07-Dec-2022	8.8	Improper authentication vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and	http://www.unimo.co.jp/table_notice/index.php?act=1&resid=1666	O-UNI-UDR--201222/4595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings. **CVE ID : CVE-2022-44620**	831567-004418	
Product: udr-ja1608_firmware					
Affected Version(s): * Up to (excluding) 71x10.1.107114.43a					
N/A	07-Dec-2022	8.8	Hidden functionality vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings. **CVE ID : CVE-2022-43464**	http://www.unimo.co.jp/table_notice/index.php?act=1&resid=1666831567-004418	O-UNI-UDR--201222/4596
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Dec-2022	8.8	OS command injection vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings. **CVE ID : CVE-2022-44606**	http://www.unimo.co.jp/table_notice/index.php?act=1&resid=1666831567-004418	O-UNI-UDR--201222/4597
Improper Authentication	07-Dec-2022	8.8	Improper authentication vulnerability in UDR-JA1604/UDR-	http://www.unimo.co.jp/table_notice/in	O-UNI-UDR--201222/4598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings. **CVE ID : CVE-2022-44620**	dex.php?act=1&resid=1666831567-004418	
Product: udr-ja1616_firmware					
Affected Version(s): * Up to (excluding) 71x10.1.107114.43a					
N/A	07-Dec-2022	8.8	Hidden functionality vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings. **CVE ID : CVE-2022-43464**	http://www.unimo.co.jp/table_notice/index.php?act=1&resid=1666831567-004418	O-UNI-UDR--201222/4599
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Dec-2022	8.8	OS command injection vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings. **CVE ID : CVE-2022-44606**	http://www.unimo.co.jp/table_notice/index.php?act=1&resid=1666831567-004418	O-UNI-UDR--201222/4600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	07-Dec-2022	8.8	Improper authentication vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings. **CVE ID : CVE-2022-44620**	http://www.unimo.co.jp/table_notice/index.php?act=1&resid=1666831567-004418	O-UNI-UDR--201222/4601
Vendor: westerndigital					
Product: my_cloud_home_duo_firmware					
Affected Version(s): * Up to (excluding) 8.12.0-178					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Dec-2022	7.8	A path traversal vulnerability was addressed in Western Digital My Cloud Home, My Cloud Home Duo and SanDisk ibi which could allow an attacker to initiate installation of custom ZIP packages and overwrite system files. This could potentially lead to a code execution. **CVE ID : CVE-2022-29837**	https://www.westerndigital.com/support/product-security/wdc-22018-western-digital-my-cloud-home-my-cloud-home-duo-and-sandisk-ibi-firmware-version-8-12-0-178	O-WES-MY_C-201222/4602
Product: my_cloud_home_firmware					
Affected Version(s): * Up to (excluding) 8.12.0-178					
Improper Limitation of a Pathname to a Restricted Directory	01-Dec-2022	7.8	A path traversal vulnerability was addressed in Western Digital My Cloud Home, My Cloud Home Duo and SanDisk ibi which could allow an attacker to	https://www.westerndigital.com/support/product-security/wdc-22018-western-	O-WES-MY_C-201222/4603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			initiate installation of custom ZIP packages and overwrite system files. This could potentially lead to a code execution. **CVE ID : CVE-2022-29837**	digital-my-cloud-home-my-cloud-home-duo-and-sandisk-ibi-firmware-version-8-12-0-178	
Product: my_cloud_os					
Affected Version(s): * Up to (excluding) 5.25.124					
Insufficiently Protected Credentials	09-Dec-2022	5.5	Insufficiently Protected Credentials vulnerability in the remote backups application on Western Digital My Cloud devices that could allow an attacker who has gained access to a relevant endpoint to use that information to access protected data. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29839**	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	O-WES-MY_C-201222/4604
Improper Authentication	09-Dec-2022	4.6	Improper Authentication vulnerability in the encrypted volumes and auto mount features of Western Digital My Cloud devices allows insecure direct access to the drive information in the case of a device reset. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux. **CVE ID : CVE-2022-29838**	https://www.westerndigital.com/support/product-security/wdc-22019-my-cloud-firmware-version-5-25-124	O-WES-MY_C-201222/4605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sandisk_ibi_firmware					
Affected Version(s): * Up to (excluding) 8.12.0-178					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Dec-2022	7.8	A path traversal vulnerability was addressed in Western Digital My Cloud Home, My Cloud Home Duo and SanDisk ibi which could allow an attacker to initiate installation of custom ZIP packages and overwrite system files. This could potentially lead to a code execution. **CVE ID : CVE-2022-29837**	https://www.westerndigital.com/support/product-security/wdc-22018-western-digital-my-cloud-home-my-cloud-home-duo-and-sandisk-ibi-firmware-version-8-12-0-178	O-WES-SAND-201222/4606
Vendor: xiongmaitech					
Product: mbd6304t_firmware					
Affected Version(s): 4.02.r11.00000117.10001.131900.00000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	O-XIO-MBD6-201222/4607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd6808t-pl_firmware					
Affected Version(s): 4.02.r11.c7431119.12001.130000.00000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	O-XIO-NBD6-201222/4608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd7004t-p_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	O-XIO-NBD7-201222/4609
Product: nbd7008t-p_firmware					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	O-XIO-NBD7-201222/4610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7016t-f-v2_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	O-XIO-NBD7-201222/4611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7024h-p_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	O-XIO-NBD7-201222/4612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7024t-p_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	O-XIO-NBD7-201222/4613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd7804r-fw_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	O-XIO-NBD7-201222/4614
Product: nbd7804r-f\(ep\)_firmware					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	O-XIO-NBD7-201222/4615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7804r-f\(hdmi\)_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	O-XIO-NBD7-201222/4616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7804t-pl_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	O-XIO-NBD7-201222/4617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7808r-pl\(ep\)_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	O-XIO-NBD7-201222/4618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd7808r-pl\(hdmi\)_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	O-XIO-NBD7-201222/4619
Product: nbd7808t-pl_firmware					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	O-XIO-NBD7-201222/4620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7904r-fs_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	O-XIO-NBD7-201222/4621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7904t-pl-xpoe_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	O-XIO-NBD7-201222/4622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7904t-plc-xpoe_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	O-XIO-NBD7-201222/4623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd7904t-pl_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	O-XIO-NBD7-201222/4624
Product: nbd7904t-p_firmware					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	O-XIO-NBD7-201222/4625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7904t-q_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	O-XIO-NBD7-201222/4626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd7908t-q_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	O-XIO-NBD7-201222/4627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8004r-pl\(ep\)_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	O-XIO-NBD8-201222/4628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd8004r-yl\(ep\)_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	O-XIO-NBD8-201222/4629
Product: nbd8004t-q_firmware					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	O-XIO-NBD8-201222/4630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8008r-pl\(ep\)_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	O-XIO-NBD8-201222/4631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8008r-pl_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	O-XIO-NBD8-201222/4632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8008r-yl\(ep\)_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	O-XIO-NBD8-201222/4633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd8008ra-glk_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	O-XIO-NBD8-201222/4634
Product: nbd8008ra-gl_firmware					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	O-XIO-NBD8-201222/4635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8008ra-ula_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	O-XIO-NBD8-201222/4636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8008ra-ulk_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	O-XIO-NBD8-201222/4637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8008ra-ul\(ep\)_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	O-XIO-NBD8-201222/4638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd8008t-q_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	O-XIO-NBD8-201222/4639
Product: nbd8009s-ula-v2_firmware					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	O-XIO-NBD8-201222/4640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8010s-kl-v2_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	O-XIO-NBD8-201222/4641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8016r-ul_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	O-XIO-NBD8-201222/4642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8016ra-k\(ep\)_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	O-XIO-NBD8-201222/4643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd8016ra-ula_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	O-XIO-NBD8-201222/4644
Product: nbd8016ra-ulk_firmware					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	O-XIO-NBD8-201222/4645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8016ra-ul\(ep\)_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	O-XIO-NBD8-201222/4646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8016ra-ul_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	O-XIO-NBD8-201222/4647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8016s-kl-v2_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	O-XIO-NBD8-201222/4648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd8016s-ula-v2_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	O-XIO-NBD8-201222/4649
Product: nbd8016t-q-v2_firmware					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	O-XIO-NBD8-201222/4650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8025r-ul_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	O-XIO-NBD8-201222/4651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8032h4-p_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	O-XIO-NBD8-201222/4652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8032h4-qe_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	O-XIO-NBD8-201222/4653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd8032h4-q_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	O-XIO-NBD8-201222/4654
Product: nbd8032h4-ul_firmware					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	O-XIO-NBD8-201222/4655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8032h8-p_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	O-XIO-NBD8-201222/4656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8032h8-qe_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	O-XIO-NBD8-201222/4657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8032ra-ul-v2_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	O-XIO-NBD8-201222/4658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd8064h8-p_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	O-XIO-NBD8-201222/4659
Product: nbd80n16ra-kl\(ep\)_firmware					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	O-XIO-NBD8-201222/4660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd80n16ra-kl_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	O-XIO-NBD8-201222/4661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd80s08s-kl\(ep\)_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	O-XIO-NBD8-201222/4662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd80s10s-kl_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	O-XIO-NBD8-201222/4663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd80s16s-kl\(ep\)_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	O-XIO-NBD8-201222/4664
Product: nbd80s16s-kl_firmware					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	O-XIO-NBD8-201222/4665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd80x09ra-kl_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	O-XIO-NBD8-201222/4666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd80x09s-kl_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	O-XIO-NBD8-201222/4667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd88x09s-kl_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	O-XIO-NBD8-201222/4668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd8904r-pl_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	O-XIO-NBD8-201222/4669
Product: nbd8904r-yl_firmware					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	O-XIO-NBD8-201222/4670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8904t-gsc-xpoe_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	O-XIO-NBD8-201222/4671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8904t-q_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	O-XIO-NBD8-201222/4672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8908r-pl_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	O-XIO-NBD8-201222/4673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Product: nbd8908r-yl_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**	N/A	O-XIO-NBD8-201222/4674
Product: nbd8908t-pl-xpoe_firmware					
Affected Version(s): -					
Improper Neutralization of Special	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.100	N/A	O-XIO-NBD8-201222/4675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			01.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8908t-plc-xpoe_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in	N/A	O-XIO-NBD8-201222/4676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8916f4-q_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system	N/A	O-XIO-NBD8-201222/4677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd. **CVE ID : CVE-2022-45045**		
Product: nbd8916f8-q_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Dec-2022	8.8	Multiple Xiongmai NVR devices, including MBD6304T V4.02.R11.00000117.10001.131900.00000 and NBD6808T-PL V4.02.R11.C7431119.12001.130000.00000, allow authenticated users to execute arbitrary commands as root, as exploited in the wild starting in approximately 2019. A remote and authenticated attacker, possibly using the default admin:tlJwpbo6 credentials, can connect to port 34567 and execute arbitrary operating system commands via a crafted JSON file during an upgrade request. Since at least 2021, Xiongmai has applied patches to prevent attackers from using this mechanism to execute telnetd.	N/A	O-XIO-NBD8-201222/4678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45045		
Vendor: yoctoproject					
Product: yocto					
Affected Version(s): 3.1					
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07453613; Issue ID: ALPS07453613. **CVE ID : CVE-2022-32631**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-YOC-YOCT-201222/4679
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-YOC-YOCT-201222/4680
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction	https://corp.mediatek.com/product-security-bulletin/December-2022	O-YOC-YOCT-201222/4681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**		
Affected Version(s): 3.3					
Improper Input Validation	05-Dec-2022	6.7	In Wi-Fi, 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. Patch ID: ALPS07441630; Issue ID: ALPS07441630. **CVE ID : CVE-2022-32632**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-YOC-YOCT-201222/4682
Improper Privilege Management	05-Dec-2022	6.7	In Wi-Fi, there is a possible memory access violation due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441637; Issue ID: ALPS07441637. **CVE ID : CVE-2022-32633**	https://corp.mediatek.com/product-security-bulletin/December-2022	O-YOC-YOCT-201222/4683
Vendor: zephyrproject					
Product: zephyr					
Affected Version(s): * Up to (including) 3.1.0					
N/A	09-Dec-2022	9.8	There is an error in the condition of the last if-statement in the function	N/A	O-ZEP-ZEPH-201222/4684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			smp_check_keys. It was rejecting current keys if all requirements were unmet. **CVE ID : CVE-2022-2993**		
Vendor: ZTE					
Product: otcp_firmware					
Affected Version(s): * Up to (excluding) 2.21.40.06					
Incorrect Permission Assignment for Critical Resource	05-Dec-2022	6.5	ZTE OTCP product is impacted by a permission and access control vulnerability. Due to improper permission settings, an attacker with high permissions could use this vulnerability to maliciously delete and modify files. **CVE ID : CVE-2022-23143**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026164	O-ZTE-OTCP-201222/4685
Vendor: Zyxel					
Product: atp100w_firmware					
Affected Version(s): From (including) 4.32 Up to (including) 5.31					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	O-ZYX-ATP1-201222/4686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**		
Product: atp100_firmware					
Affected Version(s): From (including) 4.32 Up to (including) 5.31					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	O-ZYX-ATP1-201222/4687
Product: atp200_firmware					
Affected Version(s): From (including) 4.32 Up to (including) 5.31					
Improper Neutralization of	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel	https://www.zyxel.com/global/en/suppo	O-ZYX-ATP2-201222/4688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	rt/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	
Product: atp500_firmware					
Affected Version(s): From (including) 4.32 Up to (including) 5.31					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	O-ZYX-ATP5-201222/4689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**		
Product: atp700_firmware					
Affected Version(s): From (including) 4.32 Up to (including) 5.31					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	O-ZYX-ATP7-201222/4690
Product: atp800_firmware					
Affected Version(s): From (including) 4.32 Up to (including) 5.31					
Improper Neutralization of Input During Web Page	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-	O-ZYX-ATP8-201222/4691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	advisory-for-xss-vulnerability-in-firewalls	
Product: usg40w_firmware					
Affected Version(s): From (including) 4.30 Up to (including) 4.72					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	O-ZYX-USG4-201222/4692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed on the victim's browser. **CVE ID : CVE-2022-40603**		
Product: usg40_firmware					
Affected Version(s): From (including) 4.30 Up to (including) 4.72					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	O-ZYX-USG4-201222/4693
Product: usg60w_firmware					
Affected Version(s): From (including) 4.30 Up to (including) 4.72					
Improper Neutralization of Input During Web Page Generation	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-	O-ZYX-USG6-201222/4694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	vulnerability-in-firewalls	
Product: usg60_firmware					
Affected Version(s): From (including) 4.30 Up to (including) 4.72					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	O-ZYX-USG6-201222/4695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40603		
Product: usg_flex_100w_firmware					
Affected Version(s): From (including) 4.50 Up to (including) 5.31					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	O-ZYX-USG_-201222/4696
Product: usg_flex_200_firmware					
Affected Version(s): From (including) 4.50 Up to (including) 5.31					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	O-ZYX-USG_-201222/4697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**		
Product: usg_flex_500_firmware					
Affected Version(s): From (including) 4.50 Up to (including) 5.31					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	O-ZYX-USG_-201222/4698
Product: usg_flex_50w_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.50 Up to (including) 5.31					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	O-ZYX-USG_-201222/4699
Product: usg_flex_700_firmware					
Affected Version(s): From (including) 4.50 Up to (including) 5.31					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	O-ZYX-USG_-201222/4700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**		
Product: vpn1000_firmware					
Affected Version(s): From (including) 4.30 Up to (including) 5.31					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	O-ZYX-VPN1-201222/4701
Product: vpn100_firmware					
Affected Version(s): From (including) 4.30 Up to (including) 5.31					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	O-ZYX-VPN1-201222/4702
Product: vpn300_firmware					
Affected Version(s): From (including) 4.30 Up to (including) 5.31					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	O-ZYX-VPN3-201222/4703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**		
Product: vpn50_firmware					
Affected Version(s): From (including) 4.30 Up to (including) 5.31					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in the CGI program of Zyxel ZyWALL/USG series firmware versions 4.30 through 4.72, VPN series firmware versions 4.30 through 5.31, USG FLEX series firmware versions 4.50 through 5.31, and ATP series firmware versions 4.32 through 5.31, which could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. Then, the attacker could gain access to some browser-based information if the malicious script is executed on the victim's browser. **CVE ID : CVE-2022-40603**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-xss-vulnerability-in-firewalls	O-ZYX-VPN5-201222/4704