National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
16 – 31 Oct 2023 Vol. 10 No. 20

Table of Content

Vendor	Product	Page Number
stellar	rs-stellar-strkey	1002
stephanieleary	next_page	1002
stylemixthemes	motors_-_car_dealer\,_classifieds_\&_listing	1002
Sugarcrm	sugarcrm	1003
Superwebmailer	superwebmailer	1006
syedbalkhi	wp_lightbox_2	1008
taggbox	taggbox	1008
tammersoft	shared_files	1008
task_reminder_system_project	task_reminder_system	1009
tauri	tauri	1009
technowich	wp_ulike_-_most_advanced_wordpress_marketing_toolkit	1013
Tenable	nessus_network_monitor	1014
teomantuncer	node_email_check	1015
terminalfour	terminalfour	1016
themeblvd	tweeple	1017
themepoints	super_testimonials	1017
	team_showcase	1018
themeum	tutor_lms	1019
themevolty	theme_volty_cms_blog	1020
thingnario	photon	1020
thirtybees	thirty_bees	1021
Tibco	hawk	1021
	hawk_distribution_for_tibco_silver_fabric	1022
	operational_intelligence_hawk_redtail	1023
	runtime_agent	1025
tiny	tinymce	1026
tongda2000	tongda_oa	1032
torbot_project	torbot	1037
total-soft	portfolio_gallery_responsive_image_gallery	1038
totalpress	custom_post_types	1038
tribalsystems	zenario	1038

Vendor	Product	Page Number
AMD	radeon_rx_6300m	1192
	radeon_rx_6400	1192
	radeon_rx_6450m	1193
	radeon_rx_6500m	1193
	radeon_rx_6500_xt	1194
	radeon_rx_6550m	1194
	radeon_rx_6550s	1195
	radeon_rx_6600	1195
	radeon_rx_6600m	1196
	radeon_rx_6600s	1196
	radeon_rx_6600_xt	1197
	radeon_rx_6650m	1197
	radeon_rx_6650m_xt	1198
	radeon_rx_6650_xt	1198
	radeon_rx_6700	1199
	radeon_rx_6700m	1199
	radeon_rx_6700s	1200
	radeon_rx_6700_xt	1200
	radeon_rx_6750_gre_10gb	1201
	radeon_rx_6750_gre_12gb	1201
	radeon_rx_6750_xt	1202
	radeon_rx_6800	1202
	radeon_rx_6800s	1203
	radeon_rx_6800_xt	1203
	radeon_rx_6900_xt	1204
	radeon_rx_6950_xt	1204
	radeon_rx_7600	1205
	radeon_rx_7600m	1205
	radeon_rx_7600m_xt	1206
	radeon_rx_7600s	1206
	radeon_rx_7700s	1207
	radeon_rx_7700_xt	1207

Vendor	Product	Page Number
AMD	radeon_rx_7800_xt	1208
	radeon_rx_7900m	1208
	radeon_rx_7900_gre	1209
	radeon_rx_7900_xt	1209
	radeon_rx_7900_xtx	1210
	ryzen_3_7320u	1210
	ryzen_3_7335u	1211
	ryzen_3_7440u	1211
	ryzen_5_6600h	1212
	ryzen_5_6600hs	1212
	ryzen_5_6600u	1213
	ryzen_5_7500f	1213
	ryzen_5_7520u	1214
	ryzen_5_7535hs	1214
	ryzen_5_7535u	1215
	ryzen_5_7540u	1215
	ryzen_5_7600	1216
	ryzen_5_7600x	1216
	ryzen_5_7640h	1217
	ryzen_5_7640u	1217
	ryzen_5_7645hx	1218
	ryzen_5_pro_7640hs	1218
	ryzen_5_pro_7645	1219
	ryzen_7_6800h	1219
	ryzen_7_6800hs	1220
	ryzen_7_6800u	1220
	ryzen_7_7700	1221
	ryzen_7_7700x	1221
	ryzen_7_7735hs	1222
	ryzen_7_7735u	1222
	ryzen_7_7736u	1223
	ryzen_7_7745hx	1223

Vendor	Product	Page Number
Axis	p3265-v	1242
	p3267-lv	1243
	p3267-lve	1243
	p3268-lv	1244
	p3268-lve	1245
	p3827-pve	1245
	p4705-plve	1246
	p4707-plve	1247
	q1656	1248
	q1656-b	1248
	q1656-be	1249
	q1656-ble	1250
	q1656-dle	1250
	q1656-le	1251
	q1961-te	1252
	q2101-te	1252
	q3527-lve	1253
	q3536-lve	1254
	q3538-lve	1254
	q3626-ve	1255
	q3628-ve	1256
	xfq1656	1256
bakerhughes	bentley_nevada_3500_system	1257
boschrexroth	ctrlx_hmi_web_panel_wr2107	1258
	ctrlx_hmi_web_panel_wr2110	1264
	ctrlx_hmi_web_panel_wr2115	1269
byzoro	smart_s85f	1275
Cisco	catalyst_3650	1276
	catalyst_3650-12x48fd-e	1277
	catalyst_3650-12x48fd-l	1278
	catalyst_3650-12x48fd-s	1279
	catalyst_3650-12x48uq	1279

Vendor	Product	Page Number
Cisco	catalyst_3650-12x48uq-e	1280
	catalyst_3650-12x48uq-l	1281
	catalyst_3650-12x48uq-s	1281
	catalyst_3650-12x48ur	1282
	catalyst_3650-12x48ur-e	1283
	catalyst_3650-12x48ur-l	1284
	catalyst_3650-12x48ur-s	1284
	catalyst_3650-12x48uz	1285
	catalyst_3650-12x48uz-e	1286
	catalyst_3650-12x48uz-l	1286
	catalyst_3650-12x48uz-s	1287
	catalyst_3650-24pd	1288
	catalyst_3650-24pd-e	1289
	catalyst_3650-24pd-l	1289
	catalyst_3650-24pd-s	1290
	catalyst_3650-24pdm	1291
	catalyst_3650-24pdm-e	1291
	catalyst_3650-24pdm-l	1292
	catalyst_3650-24pdm-s	1293
	catalyst_3650-24ps-e	1294
	catalyst_3650-24ps-l	1294
	catalyst_3650-24ps-s	1295
	catalyst_3650-24td-e	1296
	catalyst_3650-24td-l	1296
	catalyst_3650-24td-s	1297
	catalyst_3650-24ts-e	1298
	catalyst_3650-24ts-l	1299
	catalyst_3650-24ts-s	1299
	catalyst_3650-48fd-e	1300
	catalyst_3650-48fd-l	1301
	catalyst_3650-48fd-s	1301
	catalyst_3650-48fq	1302

Vendor	Product	Page Number
Cisco	catalyst_3650-48fq-e	1303
	catalyst_3650-48fq-l	1304
	catalyst_3650-48fq-s	1304
	catalyst_3650-48fqm	1305
	catalyst_3650-48fqm-e	1306
	catalyst_3650-48fqm-l	1306
	catalyst_3650-48fqm-s	1307
	catalyst_3650-48fs-e	1308
	catalyst_3650-48fs-l	1309
	catalyst_3650-48fs-s	1309
	catalyst_3650-48pd-e	1310
	catalyst_3650-48pd-l	1311
	catalyst_3650-48pd-s	1311
	catalyst_3650-48pq-e	1312
	catalyst_3650-48pq-l	1313
	catalyst_3650-48pq-s	1314
	catalyst_3650-48ps-e	1314
	catalyst_3650-48ps-l	1315
	catalyst_3650-48ps-s	1316
	catalyst_3650-48td-e	1316
	catalyst_3650-48td-l	1317
	catalyst_3650-48td-s	1318
	catalyst_3650-48tq-e	1319
	catalyst_3650-48tq-l	1319
	catalyst_3650-48tq-s	1320
	catalyst_3650-48ts-e	1321
	catalyst_3650-48ts-l	1321
	catalyst_3650-48ts-s	1322
	catalyst_3650-8x24pd-e	1323
	catalyst_3650-8x24pd-l	1324
	catalyst_3650-8x24pd-s	1324
	catalyst_3650-8x24uq	1325

Vendor	Product	Page Number
Cisco	catalyst_3650-8x24uq-e	1326
	catalyst_3650-8x24uq-l	1326
	catalyst_3650-8x24uq-s	1327
	catalyst_3850	1328
	catalyst_3850-12s-e	1329
	catalyst_3850-12s-s	1329
	catalyst_3850-12x48u	1330
	catalyst_3850-12xs-e	1331
	catalyst_3850-12xs-s	1331
	catalyst_3850-16xs-e	1332
	catalyst_3850-16xs-s	1333
	catalyst_3850-24p-e	1334
	catalyst_3850-24p-l	1334
	catalyst_3850-24p-s	1335
	catalyst_3850-24pw-s	1336
	catalyst_3850-24s-e	1336
	catalyst_3850-24s-s	1337
	catalyst_3850-24t-e	1338
	catalyst_3850-24t-l	1339
	catalyst_3850-24t-s	1339
	catalyst_3850-24u	1340
	catalyst_3850-24u-e	1341
	catalyst_3850-24u-l	1341
	catalyst_3850-24u-s	1342
	catalyst_3850-24xs	1343
	catalyst_3850-24xs-e	1344
	catalyst_3850-24xs-s	1344
	catalyst_3850-24xu	1345
	catalyst_3850-24xu-e	1346
	catalyst_3850-24xu-l	1346
	catalyst_3850-24xu-s	1347
	catalyst_3850-32xs-e	1348

Vendor	Product	Page Number
Cisco	catalyst_3850-32xs-s	1349
	catalyst_3850-48f-e	1349
	catalyst_3850-48f-l	1350
	catalyst_3850-48f-s	1351
	catalyst_3850-48p-e	1351
	catalyst_3850-48p-l	1352
	catalyst_3850-48p-s	1353
	catalyst_3850-48pw-s	1354
	catalyst_3850-48t-e	1354
	catalyst_3850-48t-l	1355
	catalyst_3850-48t-s	1356
	catalyst_3850-48u	1356
	catalyst_3850-48u-e	1357
	catalyst_3850-48u-l	1358
	catalyst_3850-48u-s	1359
	catalyst_3850-48xs	1359
	catalyst_3850-48xs-e	1360
	catalyst_3850-48xs-f-e	1361
	catalyst_3850-48xs-f-s	1361
	catalyst_3850-48xs-s	1362
	catalyst_3850-nm-2-40g	1363
	catalyst_3850-nm-8-10g	1364
contec	solarview_compact	1364
Dlink	dar-7000	1365
	di-7003g	1366
	di-7100g	1372
	di-7100g\+	1378
	di-7200g	1385
	di-7200g\+	1391
	di-7300g\+	1398
	di-7400g\+	1404
	dir-820l	1410

Vendor	Product	Page Number
Dlink	dsl-2730u	1411
	dsl-2750u	1411
Eaton	easy-box-e4-ac1	1412
	easy-box-e4-dc1	1412
	easy-box-e4-uc1	1413
	easy-e4-ac-12rc1p	1413
	easy-e4-ac-12rcx1p	1414
	easy-e4-ac-16re1p	1415
	easy-e4-dc-12tc1p	1415
	easy-e4-dc-12tcx1p	1416
	easy-e4-dc-16te1p	1416
	easy-e4-dc-4pe1p	1417
	easy-e4-dc-6ae1p	1417
	easy-e4-dc-8te1p	1418
	easy-e4-uc-12rc1p	1419
	easy-e4-uc-12rcx1p	1419
	easy-e4-uc-16re1	1420
	easy-e4-uc-16re1p	1420
	easy-e4-uc-8re1p	1421
	easy_e4-ac-8re1p	1421
	xv-102-a035tqrb-1e4	1422
	xv-102-a3-57tvrb-1e4	1422
	xv100-box-e4-dc1	1423
	xv100-box-e4-uc1	1424
govee	led_strip	1424
HP	200_g4_22_all-in-one_pc_\(rom_family_ssid_86f0\)	1425
	200_g4_22_all-in-one_pc_\(rom_family_ssid_86f2\)	1425
	200_g4_22_all-in-one_pc_\(rom_family_ssid_86f3\)	1425
	200_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f0\)	1426

Vendor	Product	Page Number
HP	200_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f2\)	1426
	200_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f3\)	1427
	205_g4_22_all-in-one_pc_\(rom_family_ssid_86f0\)	1427
	205_g4_22_all-in-one_pc_\(rom_family_ssid_86f2\)	1427
	205_g4_22_all-in-one_pc_\(rom_family_ssid_86f3\)	1428
	205_g8_24_all-in-one_pc_\(rom_family_ssid_8923\)	1428
	205_g8_24_all-in-one_pc_\(rom_family_ssid_8924\)	1429
	205_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f0\)	1429
	205_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f2\)	1430
	205_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f3\)	1430
	205_pro_g8_24_all-in-one_pc_\(rom_family_ssid_8923\)	1430
	205_pro_g8_24_all-in-one_pc_\(rom_family_ssid_8924\)	1431
	240_g10	1431
	240_g6	1432
	240_g7	1432
	240_g9	1433
	245	1433
	245_g10	1433
	245_g7	1434
	245_g8	1434
	245_g9	1435
	246_g6	1435
	246_g7	1435

Vendor	Product	Page Number
HP	desktop_pro_a_g3_microtower	1448
	proone_240_g10_\(rom_family_ssid_8b4c\)	1449
	proone_240_g10_\(rom_family_ssid_8b4d\)	1449
	proone_240_g9_\(rom_family_ssid_89eb\)	1449
	pro_sff_280_g9_desktop_\(rom_family_ssid_89b4\)	1450
	pro_sff_280_g9_desktop_\(rom_family_ssid_8bc3\)	1450
	pro_sff_290_g9_desktop_\(rom_family_ssid_89b4\)	1451
	pro_sff_290_g9_desktop_\(rom_family_ssid_8bc3\)	1451
	pro_sff_zhan_66_g9_desktop_\(rom_family_ssid_89b4\)	1451
	pro_sff_zhan_66_g9_desktop_\(rom_family_ssid_8bc3\)	1452
	pro_tower_200_g9_desktop_\(rom_family_ssid_89b3\)	1452
	pro_tower_200_g9_desktop_\(rom_family_ssid_89b4\)	1453
	pro_tower_200_g9_desktop_\(rom_family_ssid_8bc3\)	1453
	pro_tower_280_g9_desktop_\(rom_family_ssid_89b3\)	1454
	pro_tower_280_g9_desktop_\(rom_family_ssid_89b4\)	1454
	pro_tower_290_g9_desktop_\(rom_family_ssid_89b3\)	1454
	pro_tower_290_g9_desktop_\(rom_family_ssid_89b4\)	1455
	pro_tower_290_g9_desktop_\(rom_family_ssid_8bc3\)	1455
	pro_tower_zhan_99_g9_desktop_\(rom_family_ssid_89b3\)	1456
	pro_tower_zhan_99_g9_desktop_\(rom_family_ssid_89b4\)	1456

Vendor	Product	Page Number
HP	pro_tower_zhan_99_g9_desktop_\(rom_family_ssid_8b3c\)	1457
	stream_11_pro_g4	1457
	stream_11_pro_g5	1457
	t638_thin_client	1458
	vr_backpack_g2_\(rom_family_ssid_8590\)	1458
	zbook_15_g5_mobile_workstation	1459
	zhan_66_pro_a_g10_\(rom_family_ssid_8b4e\)	1459
	zhan_66_pro_a_g1_r_microtower	1459
	zhan_66_pro_a_g4_all-in-one_pc_\(rom_family_ssid_8923\)	1460
	zhan_66_pro_a_g4_all-in-one_pc_\(rom_family_ssid_8924\)	1460
	zhan_99_g3_mobile_workstation	1461
	zhan_99_g4_mobile_workstation	1461
	zhan_99_pro_a_g2_microtower_\(rom_family_ssid_871e\)	1462
hpe	alletra_4110	1462
	alletra_4120	1462
	alletra_4140	1463
	apollo_2000_system	1463
	apollo_4200_gen10_plus_system	1463
	apollo_4200_gen10_server	1463
	apollo_4510_gen10_system	1464
	apollo_6500_gen10_plus_system	1464
	apollo_6500_gen10_system	1464
	apollo_n2600_gen10_plus	1464
	apollo_n2800_gen10_plus	1465
	apollo_r2200_gen10	1465
	apollo_r2600_gen10	1465
	apollo_r2800_gen10	1465
	edgeline_e920d_server_blade	1466
	edgeline_e920t_server_blade	1466

Vendor	Product	Page Number
hpe	edgeline_e920_server_blade	1466
	proliant_bl460c_gen10_server_blade	1466
	proliant_dl110_gen10_plus_telco_server	1467
	proliant_dl110_gen11	1467
	proliant_dl160_gen10_server	1467
	proliant_dl180_gen10_server	1468
	proliant_dl20_gen10_plus_server	1468
	proliant_dl20_gen10_server	1468
	proliant_dl20_gen11	1468
	proliant_dl320_gen11_server	1469
	proliant_dl325_gen10_plus_server	1469
	proliant_dl325_gen10_plus_v2_server	1469
	proliant_dl325_gen11_server	1469
	proliant_dl345_gen10_plus_server	1470
	proliant_dl345_gen11_server	1470
	proliant_dl360_gen10_plus_server	1470
	proliant_dl360_gen10_server	1470
	proliant_dl360_gen11_server	1471
	proliant_dl365_gen10_plus_server	1471
	proliant_dl365_gen11_server	1471
	proliant_dl380a_gen11	1471
	proliant_dl380_gen10_plus_server	1472
	proliant_dl380_gen10_server	1472
	proliant_dl380_gen11_server	1472
	proliant_dl385_gen10_plus_server	1472
	proliant_dl385_gen10_plus_v2_server	1473
	proliant_dl385_gen10_server	1473
	proliant_dl385_gen11_server	1473
	proliant_dl560_gen10_server	1474
	proliant_dl560_gen11	1474
	proliant_dl580_gen10_server	1474
	proliant_e910t_server_blade	1474

Vendor	Product	Page Number
hpe	proliant_e910_server_blade	1475
	proliant_m750_server_blade	1475
	proliant_microserver_gen10_plus	1475
	proliant_microserver_gen10_plus_v2	1475
	proliant_ml110_gen10_server	1476
	proliant_ml110_gen11	1476
	proliant_ml30_gen10_plus_server	1476
	proliant_ml30_gen10_server	1476
	proliant_ml30_gen11	1477
	proliant_ml350_gen10_server	1477
	proliant_ml350_gen11_server	1477
	proliant_rl300_gen11	1477
	proliant_xl170r_gen10_server	1478
	proliant_xl190r_gen10_server	1478
	proliant_xl220n_gen10_plus_server	1478
	proliant_xl225n_gen10_plus_1u_node	1478
	proliant_xl230k_gen10_server	1479
	proliant_xl270d_gen10_server	1479
	proliant_xl290n_gen10_plus_server	1479
	proliant_xl2x260w_gen10_server	1480
	proliant_xl645d_gen10_plus_server	1480
	proliant_xl675d_gen10_plus_server	1480
	proliant_xl925g_gen10_plus_1u_4-node_configure-to-order_server	1480
	synergy_480_gen10_compute_module	1481
	synergy_480_gen10_plus_compute_module	1481
	synergy_480_gen11_compute_module	1481
	synergy_660_gen10_compute_module	1481
Lenovo	thinkagile_hx1021_edg	1482
	thinkagile_hx1320	1482
	thinkagile_hx1321	1482
	thinkagile_hx1331	1483
	thinkagile_hx1520-r	1484

Vendor	Product	Page Number
Lenovo	thinkagile_hx1521-r	1484
	thinkagile_hx2320-e	1484
	thinkagile_hx2321	1485
	thinkagile_hx2330	1485
	thinkagile_hx2331	1486
	thinkagile_hx2720-e	1487
	thinkagile_hx3320	1487
	thinkagile_hx3321	1488
	thinkagile_hx3330	1488
	thinkagile_hx3331	1489
	thinkagile_hx3375	1490
	thinkagile_hx3376	1491
	thinkagile_hx3520-g	1493
	thinkagile_hx3521-g	1493
	thinkagile_hx3720	1493
	thinkagile_hx3721	1493
	thinkagile_hx5520	1494
	thinkagile_hx5520-c	1494
	thinkagile_hx5521	1494
	thinkagile_hx5521-c	1495
	thinkagile_hx5530	1495
	thinkagile_hx5531	1496
	thinkagile_hx7520	1497
	thinkagile_hx7521	1498
	thinkagile_hx7530	1498
	thinkagile_hx7531	1499
	thinkagile_hx7820	1500
	thinkagile_hx7821	1500
	thinkagile_hx_enclosure	1501
	thinkagile_mx1021_on_se350	1501
	thinkagile_mx3330-f_all-flash	1501
	thinkagile_mx3330-h_hybrid	1502

Vendor	Product	Page Number
Lenovo	thinkagile_mx3331-f_all-flash	1504
	thinkagile_mx3331-h_hybrid	1505
	thinkagile_mx3530-h_hybrid	1506
	thinkagile_mx3530_f_all_flash	1507
	thinkagile_mx3531-f_all-flash	1508
	thinkagile_mx3531_h_hybrid	1510
	thinkagile_mx630_v3_firmware	1511
	thinkagile_mx630_v3_intergrated_system_firmware	1511
	thinkagile_mx650_v3_firmware	1511
	thinkagile_mx650_v3_intergrated_system_firmware	1512
	thinkagile_mx_edge-_mx1020_	1512
	thinkagile_vx1320	1512
	thinkagile_vx2320	1512
	thinkagile_vx2330	1513
	thinkagile_vx3320	1514
	thinkagile_vx3330	1514
	thinkagile_vx3331	1515
	thinkagile_vx3520-g	1517
	thinkagile_vx3530-g	1517
	thinkagile_vx3720	1518
	thinkagile_vx5520	1518
	thinkagile_vx5530	1519
	thinkagile_vx7320_n	1520
	thinkagile_vx7330	1520
	thinkagile_vx7520	1521
	thinkagile_vx7520_n	1521
	thinkagile_vx7530	1522
	thinkagile_vx7531	1523
	thinkagile_vx7820	1524
	thinkagile_vx_1se	1524
	thinkagile_vx_2u4n	1525

Vendor	Product	Page Number
Lenovo	thinkagile_vx_4u	1525
	thinkedge_se450	1525
	thinkpad_t14_gen_3	1525
	thinkserver_sr590	1526
	thinksystem_sd530	1526
	thinksystem_sd630_v2	1526
	thinksystem_sd650-n_v2	1528
	thinksystem_sd650_dual_node_tray	1529
	thinksystem_sd650_dwc_dual_node_tray	1529
	thinksystem_sd650_v2	1529
	thinksystem_se350	1530
	thinksystem_sn550	1531
	thinksystem_sn550_v2	1531
	thinksystem_sn850	1532
	thinksystem_sr150	1532
	thinksystem_sr158	1533
	thinksystem_sr250	1533
	thinksystem_sr250_v2	1533
	thinksystem_sr258	1534
	thinksystem_sr258_v2	1535
	thinksystem_sr530	1536
	thinksystem_sr550	1536
	thinksystem_sr570	1536
	thinksystem_sr630	1537
	thinksystem_sr630_v2	1537
	thinksystem_sr645	1538
	thinksystem_sr645_v3	1539
	thinksystem_sr650	1541
	thinksystem_sr650_v2	1541
	thinksystem_sr665	1542
	thinksystem_sr670	1543
	thinksystem_sr670_v2	1544

Vendor	Product	Page Number
Lenovo	thinksystem_sr850	1546
	thinksystem_sr850p	1546
	thinksystem_sr850_v2	1546
	thinksystem_sr860	1547
	thinksystem_sr860_v2	1547
	thinksystem_sr950	1549
	thinksystem_st250	1549
	thinksystem_st250_v2	1549
	thinksystem_st258	1550
	thinksystem_st258_v2	1551
	thinksystem_st550	1552
	thinksystem_st650_v2	1552
	thinksystem_st658_v2	1553
Mercurycom	a15	1554
nanoleaf	lightstrip	1555
netmodule	nb1601	1555
	nb1800	1556
	nb1810	1557
	nb2800	1558
	nb2810	1559
	nb3701	1560
	nb3800	1561
	ng800	1562
nxp	i.mx_8m	1563
	i.mx_8m_mini	1564
	i.mx_8m_nano	1564
	i.mx_8m_plus	1565
sick	fx0-gent00000	1566
	fx0-gent00010	1566
	fx0-gent00030	1567
	fx0-gepr00000	1568
	fx0-gepr00010	1568

Vendor	Product	Page Number
Sonicwall	nsa_2650	1632
	nsa_3600	1635
	nsa_3650	1637
	nsa_4600	1640
	nsa_4650	1642
	nsa_5600	1645
	nsa_5650	1647
	nsa_6600	1650
	nsa_6650	1652
	nssp10700	1655
	nssp11700	1657
	nssp13700	1660
	nssp15700	1662
	nsv10	1665
	nsv100	1667
	nsv1600	1670
	nsv200	1672
	nsv25	1675
	nsv270	1677
	nsv300	1680
	nsv400	1682
	nsv470	1685
	nsv50	1687
	nsv800	1690
	nsv870	1692
	sm_9200	1695
	sm_9250	1697
	sm_9400	1700
	sm_9450	1702
	sm_9600	1705
	sm_9650	1707
	sohow	1710

Vendor	Product	Page Number
Sonicwall	soho_250	1712
	soho_250w	1715
	tz270	1717
	tz270w	1720
	tz370	1722
	tz370w	1725
	tz470	1727
	tz470w	1730
	tz570	1732
	tz570p	1735
	tz570w	1737
	tz670	1740
	tz_300	1742
	tz_300p	1745
	tz_300w	1747
	tz_350	1750
	tz_400	1752
	tz_400w	1755
	tz_500	1757
	tz_500w	1760
	tz_600	1762
	tz_600p	1765
Synology	bc500	1767
	tc500	1768
Tenda	w18e	1769
totolink	a3300r	1769
	a3700r	1770
	a7000r	1770
	cp300\+	1771
	lr1200gb	1773
	nr1800x	1773
	x2000r	1773

Vendor	Product	Page Number
totolink	x5000r	1780
	x6000r	1781
Tp-link	tl-wdr7660	1787
	tl-wr886n	1787
ui	unifi_dream_machine	1791
	unifi_dream_machine_pro	1792
	unifi_dream_machine_special_edition	1793
	unifi_dream_router	1794
	unifi_dream_wall	1795
viessmann	vitogate_300	1796
Wago	compact_controller_100	1797
	edge_controller	1797
	pfc100	1798
	pfc200	1798
	touch_panel_600_advanced	1799
	touch_panel_600_marine	1799
	touch_panel_600_standard	1800
weintek	cmt-fhd	1800
	cmt-hdm	1801
	cmt3071	1802
	cmt3072	1804
	cmt3090	1805
	cmt3103	1806
	cmt3151	1807
Yealink	sip-t19p-e2	1808
zioncom	a7000r	1808
Operating System		
airtel	dragon_path_707gr1_firmware	1809
Apple	ipados	1810
	iphone_os	1826
	macos	1841
	mac_os_x	1866

Vendor	Product	Page Number
Apple	tvos	1868
	watchos	1870
Axis	axis_os	1875
	axis_os_2016	1880
	axis_os_2018	1880
	axis_os_2020	1881
	axis_os_2022	1882
bakerhughes	bentley_nevada_3500_system_firmware	1883
boschrexroth	ctrlx_hmi_web_panel_wr2107_firmware	1884
	ctrlx_hmi_web_panel_wr2110_firmware	1889
	ctrlx_hmi_web_panel_wr2115_firmware	1895
byzoro	smart_s85f_firmware	1900
Cisco	ios_xe	1902
contec	solarview_compact_firmware	1906
Debian	debian_linux	1906
Dlink	dar-7000_firmware	1923
	di-7003g_firmware	1924
	di-7100g\+_firmware	1930
	di-7100g_firmware	1937
	di-7200g\+_firmware	1943
	di-7200g_firmware	1949
	di-7300g\+_firmware	1956
	di-7400g\+_firmware	1962
	dir-820l_firmware	1969
	dsl-2730u_firmware	1969
	dsl-2750u_firmware	1970
Eaton	easy-box-e4-ac1_firmware	1970
	easy-box-e4-dc1_firmware	1971
	easy-box-e4-uc1_firmware	1971
	easy-e4-ac-12rc1p_firmware	1972
	easy-e4-ac-12rcx1p_firmware	1972
	easy-e4-ac-16re1p_firmware	1973

Vendor	Product	Page Number
Eaton	easy-e4-dc-12tc1p_firmware	1973
	easy-e4-dc-12tcx1p_firmware	1974
	easy-e4-dc-16te1p_firmware	1975
	easy-e4-dc-4pe1p_firmware	1975
	easy-e4-dc-6ae1p_firmware	1976
	easy-e4-dc-8te1p_firmware	1976
	easy-e4-uc-12rc1p_firmware	1977
	easy-e4-uc-12rcx1p_firmware	1977
	easy-e4-uc-16re1p_firmware	1978
	easy-e4-uc-16re1_firmware	1978
	easy-e4-uc-8re1p_firmware	1979
	easy_e4-ac-8re1p_firmware	1980
	xv-102-a035tqrb-1e4_firmware	1980
	xv-102-a3-57tvrb-1e4_firmware	1981
	xv100-box-e4-dc1_firmware	1981
	xv100-box-e4-uc1_firmware	1982
Extremenetworks	exos	1982
Fedoraproject	fedora	1987
freshtomato	freshtomato	1996
Google	android	1997
govee	led_strip_firmware	2077
HP	200_g4_22_all-in-one_pc_\(rom_family_ssid_86f0\)_firmware	2077
	200_g4_22_all-in-one_pc_\(rom_family_ssid_86f2\)_firmware	2078
	200_g4_22_all-in-one_pc_\(rom_family_ssid_86f3\)_firmware	2078
	200_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f0\)_firmware	2078
	200_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f2\)_firmware	2079
	200_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f3\)_firmware	2079

Vendor	Product	Page Number
HP	205_g4_22_all-in-one_pc_\(rom_family_ssid_86f0\)_firmware	2080
	205_g4_22_all-in-one_pc_\(rom_family_ssid_86f2\)_firmware	2080
	205_g4_22_all-in-one_pc_\(rom_family_ssid_86f3\)_firmware	2081
	205_g8_24_all-in-one_pc_\(rom_family_ssid_8923\)_firmware	2081
	205_g8_24_all-in-one_pc_\(rom_family_ssid_8924\)_firmware	2081
	205_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f0\)_firmware	2082
	205_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f2\)_firmware	2082
	205_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f3\)_firmware	2083
	205_pro_g8_24_all-in-one_pc_\(rom_family_ssid_8923\)_firmware	2083
	205_pro_g8_24_all-in-one_pc_\(rom_family_ssid_8924\)_firmware	2084
	240_g10_firmware	2084
	240_g6_firmware	2084
	240_g7_firmware	2085
	240_g9_firmware	2085
	245_firmware	2086
	245_g10_firmware	2086
	245_g7_firmware	2086
	245_g8_firmware	2087
	245_g9_firmware	2087
	246_g6_firmware	2088
	246_g7_firmware	2088
	247_g8_firmware	2089
	250_g10_firmware	2089
	250_g6_firmware	2089
	250_g7_firmware	2090

Vendor	Product	Page Number
HP	250_g9_firmware	2090
	255_g10_firmware	2091
	255_g6_firmware	2091
	255_g7_firmware	2092
	255_g8_firmware	2092
	255_g8_\(rom_family_ssid_87d1\)_firmware	2092
	255_g8_\(rom_family_ssid_8905\)_firmware	2093
	255_g8_\(rom_family_ssid_890e\)_firmware	2093
	255_g9_firmware	2094
	256_g6_firmware	2094
	256_g7_firmware	2094
	258_g6_firmware	2095
	258_g7_firmware	2095
	285_g6_microtower_\(rom_family_ssid_871e\)_firmware	2096
	285_g8_microtower_\(rom_family_ssid_870e\)_firmware	2096
	285_pro_g6_microtower_\(rom_family_ssid_871e\)_firmware	2097
	285_pro_g8_microtower_\(rom_family_ssid_870e\)_firmware	2097
	295_g8_microtower_\(rom_family_ssid_870e\)_firmware	2097
	340_g7_firmware	2098
	348_g7_firmware	2098
	470_g10_firmware	2099
	470_g7_firmware	2099
	470_g9_firmware	2100
	desktop_pro_a_300_g3_firmware	2100
	desktop_pro_a_g3_firmware	2100
	desktop_pro_a_g3_microtower_firmware	2101
	proone_240_g10_\(rom_family_ssid_8b4c\)_firmware	2101

Vendor	Product	Page Number
HP	proone_240_g10_\(rom_family_ssid_8b4d\)_firmware	2102
	proone_240_g9_\(rom_family_ssid_89eb\)_firmware	2102
	pro_sff_280_g9_desktop_\(rom_family_ssid_89b4\)_firmware	2102
	pro_sff_280_g9_desktop_\(rom_family_ssid_8bc3\)_firmware	2103
	pro_sff_290_g9_desktop_\(rom_family_ssid_89b4\)_firmware	2103
	pro_sff_290_g9_desktop_\(rom_family_ssid_8bc3\)_firmware	2104
	pro_sff_zhan_66_g9_desktop_\(rom_family_ssid_89b4\)_firmware	2104
	pro_sff_zhan_66_g9_desktop_\(rom_family_ssid_8bc3\)_firmware	2105
	pro_tower_200_g9_desktop_\(rom_family_ssid_89b3\)_firmware	2105
	pro_tower_200_g9_desktop_\(rom_family_ssid_89b4\)_firmware	2105
	pro_tower_200_g9_desktop_\(rom_family_ssid_8bc3\)_firmware	2106
	pro_tower_280_g9_desktop_\(rom_family_ssid_89b3\)_firmware	2106
	pro_tower_280_g9_desktop_\(rom_family_ssid_89b4\)_firmware	2107
	pro_tower_290_g9_desktop_\(rom_family_ssid_89b3\)_firmware	2107
	pro_tower_290_g9_desktop_\(rom_family_ssid_89b4\)_firmware	2108
	pro_tower_290_g9_desktop_\(rom_family_ssid_8bc3\)_firmware	2108
	pro_tower_zhan_99_g9_desktop_\(rom_family_ssid_89b3\)_firmware	2108
	pro_tower_zhan_99_g9_desktop_\(rom_family_ssid_89b4\)_firmware	2109

Vendor	Product	Page Number
HP	pro_tower_zhan_99_g9_desktop_\(rom_family_ssid_8b3c\)_firmware	2109
	stream_11_pro_g4_firmware	2110
	stream_11_pro_g5_firmware	2110
	t638_thin_client_firmware	2110
	vr_backpack_g2_\(rom_family_ssid_8590\)_firmware	2111
	zbook_15_g5_mobile_workstation_firmware	2111
	zhan_66_pro_a_g10_\(rom_family_ssid_8b4e\)_firmware	2112
	zhan_66_pro_a_g1_r_microtower_firmware	2112
	zhan_66_pro_a_g4_all-in-one_pc_\(rom_family_ssid_8923\)_firmware	2113
	zhan_66_pro_a_g4_all-in-one_pc_\(rom_family_ssid_8924\)_firmware	2113
	zhan_99_g3_mobile_workstation_firmware	2113
	zhan_99_g4_mobile_workstation_firmware	2114
	zhan_99_pro_a_g2_microtower_\(rom_family_ssid_871e\)_firmware	2114
hpe	integrated_lights-out_5_firmware	2115
	integrated_lights-out_6_firmware	2115
IBM	aix	2115
	i	2116
Lenovo	thinkagile_hx1021_edg_firmware	2121
	thinkagile_hx1320_firmware	2121
	thinkagile_hx1321_firmware	2122
	thinkagile_hx1331_firmware	2122
	thinkagile_hx1520-r_firmware	2123
	thinkagile_hx1521-r_firmware	2123
	thinkagile_hx2320-e_firmware	2124
	thinkagile_hx2321_firmware	2124
	thinkagile_hx2330_firmware	2124
	thinkagile_hx2331_firmware	2125
	thinkagile_hx2720-e_firmware	2127

Vendor	Product	Page Number
Lenovo	thinkagile_hx3320_firmware	2127
	thinkagile_hx3321_firmware	2127
	thinkagile_hx3330_firmware	2127
	thinkagile_hx3331_firmware	2129
	thinkagile_hx3375_firmware	2130
	thinkagile_hx3376_firmware	2131
	thinkagile_hx3520-g_firmware	2132
	thinkagile_hx3521-g_firmware	2132
	thinkagile_hx3720_firmware	2132
	thinkagile_hx3721_firmware	2133
	thinkagile_hx5520-c_firmware	2133
	thinkagile_hx5520_firmware	2133
	thinkagile_hx5521-c_firmware	2134
	thinkagile_hx5521_firmware	2134
	thinkagile_hx5530_firmware	2134
	thinkagile_hx5531_firmware	2135
	thinkagile_hx7520_firmware	2137
	thinkagile_hx7521_firmware	2137
	thinkagile_hx7530_firmware	2137
	thinkagile_hx7531_firmware	2138
	thinkagile_hx7820_firmware	2140
	thinkagile_hx7821_firmware	2140
	thinkagile_hx_enclosure_firmware	2140
	thinkagile_mx1021_on_se350_firmware	2140
	thinkagile_mx3330-f_all-flash_firmware	2141
	thinkagile_mx3330-h_hybrid_firmware	2142
	thinkagile_mx3331-f_all-flash_firmware	2143
	thinkagile_mx3331-h_hybrid_firmware	2144
	thinkagile_mx3530-h_hybrid_firmware	2145
	thinkagile_mx3530_f_all_flash_firmware	2147
	thinkagile_mx3531-f_all-flash_firmware	2148
	thinkagile_mx3531_h_hybrid_firmware	2149

Vendor	Product	Page Number
Lenovo	thinkagile_mx_edge-_mx1020__firmware	2150
	thinkagile_vx1320_firmware	2150
	thinkagile_vx2320_firmware	2151
	thinkagile_vx2330_firmware	2151
	thinkagile_vx3320_firmware	2152
	thinkagile_vx3330_firmware	2152
	thinkagile_vx3331_firmware	2153
	thinkagile_vx3520-g_firmware	2154
	thinkagile_vx3530-g_firmware	2155
	thinkagile_vx3720_firmware	2156
	thinkagile_vx5520_firmware	2156
	thinkagile_vx5530_firmware	2156
	thinkagile_vx7320_n_firmware	2158
	thinkagile_vx7330_firmware	2158
	thinkagile_vx7520_firmware	2159
	thinkagile_vx7520_n_firmware	2159
	thinkagile_vx7530_firmware	2160
	thinkagile_vx7531_firmware	2161
	thinkagile_vx7820_firmware	2162
	thinkagile_vx_1se_firmware	2162
	thinkagile_vx_2u4n_firmware	2162
	thinkagile_vx_4u_firmware	2163
	thinkedge_se450__firmware	2163
	thinksystem_sd530_firmware	2163
	thinksystem_sd630_v2_firmware	2163
	thinksystem_sd650-n_v2_firmware	2165
	thinksystem_sd650_dual_node_tray_firmware	2166
	thinksystem_sd650_dwc_dual_node_tray_firmware	2166
	thinksystem_sd650_v2_firmware	2166
	thinksystem_sd650_v3_firmware	2167
	thinksystem_sd665_v3_firmware	2169
	thinksystem_se350_firmware	2170

Vendor	Product	Page Number
Lenovo	thinksystem_sn550_firmware	2170
	thinksystem_sn550_v2_firmware	2170
	thinksystem_sn850_firmware	2171
	thinksystem_sr150_firmware	2172
	thinksystem_sr158_firmware	2172
	thinksystem_sr250_firmware	2172
	thinksystem_sr258_firmware	2173
	thinksystem_sr258_v2_firmware	2174
	thinksystem_sr530_firmware	2175
	thinksystem_sr550_firmware	2175
	thinksystem_sr570_firmware	2175
	thinksystem_sr590_firmware	2176
	thinksystem_sr630_firmware	2176
	thinksystem_sr630_v2_firmware	2176
	thinksystem_sr630_v3_firmware	2177
	thinksystem_sr635_v3_firmware	2179
	thinksystem_sr645_firmware	2180
	thinksystem_sr645_v3_firmware	2181
	thinksystem_sr650_firmware	2182
	thinksystem_sr650_v2_firmware	2182
	thinksystem_sr650_v3_firmware	2184
	thinksystem_sr655_v3_firmware	2185
	thinksystem_sr665_firmware	2186
	thinksystem_sr665_v3_firmware	2187
	thinksystem_sr670_firmware	2188
	thinksystem_sr670_v2_firmware	2189
	thinksystem_sr675_v3_firmware	2191
	thinksystem_sr850p_firmware	2192
	thinksystem_sr850_firmware	2192
	thinksystem_sr850_v2_firmware	2192
	thinksystem_sr850_v3_firmware	2193
	thinksystem_sr860_firmware	2195

Vendor	Product	Page Number
sick	fx0-gpnt00030_firmware	2243
sielco	analog_fm_transmitter_exc1000gt_firmware	2244
	analog_fm_transmitter_exc1000gx_firmware	2246
	analog_fm_transmitter_exc100gt_firmware	2247
	analog_fm_transmitter_exc120gt_firmware	2249
	analog_fm_transmitter_exc120gx_firmware	2251
	analog_fm_transmitter_exc1600gx_firmware	2252
	analog_fm_transmitter_exc2000gx_firmware	2254
	analog_fm_transmitter_exc3000gx_firmware	2256
	analog_fm_transmitter_exc300gt_firmware	2258
	analog_fm_transmitter_exc300gx_firmware	2259
	analog_fm_transmitter_exc30gt_firmware	2261
	analog_fm_transmitter_exc5000gt_firmware	2263
	analog_fm_transmitter_exc5000gx_firmware	2264
	polyeco1000_firmware	2266
	polyeco300_firmware	2276
	polyeco500_firmware	2284
	radio_link_exc19_firmware	2289
	radio_link_rtx19_firmware	2291
Sonicwall	sonicos	2293
Synology	bc500_firmware	2300
	tc500_firmware	2301
Tenda	w18e_firmware	2301
totolink	a3300r_firmware	2302
	a3700r_firmware	2302
	a7000r_firmware	2303
	cp300\+_firmware	2304
	lr1200gb_firmware	2305
	nr1800x_firmware	2306
	x2000r_firmware	2306
	x5000r_firmware	2312
	x6000r_firmware	2314

Vendor	Product	Page Number
Tp-link	tl-wdr7660_firmware	2319
	tl-wr886n_firmware	2320
viessmann	vitogate_300_firmware	2324
Wago	compact_controller_100_firmware	2325
	edge_controller_firmware	2325
	pfc100_firmware	2326
	pfc200_firmware	2326
	touch_panel_600_advanced_firmware	2327
	touch_panel_600_marine_firmware	2327
	touch_panel_600_standard_firmware	2328
weintek	cmt-fhd_firmware	2328
	cmt-hdm_firmware	2329
	cmt3071_firmware	2331
	cmt3072_firmware	2332
	cmt3090_firmware	2333
	cmt3103_firmware	2334
	cmt3151_firmware	2335
Yealink	sip-t19p-e2_firmware	2336
zephyrproject	zephyr	2337
zioncom	a7000r_firmware	2337
zpesystems	nodegrid_os	2338

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 01generator					
Product: pireospay					
Affected Version(s): * Up to (excluding) 1.7.10					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Oct-2023	8.8	In the module "PireosPay" (pireospay) before version 1.7.10 from 01generator.com for PrestaShop, a guest can perform SQL injection via `PireosPayValidationModuleFrontController::postProcess().` **CVE ID : CVE-2023-45375**	https://security.friendsofpresta.org/modules/2023/10/12/pireospay.html	A-01G-PIRE-231123/1
Vendor: 100plugins					
Product: open_user_map					
Affected Version(s): * Up to (excluding) 1.3.27					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in 100plugins Open User Map plugin <= 1.3.26 versions. **CVE ID : CVE-2023-45056**	N/A	A-100-OPEN-231123/2
Vendor: 10quality					
Product: post_gallery					
Affected Version(s): * Up to (including) 2.3.12					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in 10 Quality Post	N/A	A-10Q-POST-231123/3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gallery plugin <= 2.3.12 versions. **CVE ID : CVE-2023-45752**		
Vendor: 10web					
Product: form_maker					
Affected Version(s): * Up to (excluding) 1.15.19					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in 10Web Form Builder Team Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder plugin <= 1.15.18 versions. **CVE ID : CVE-2023-45070**	N/A	A-10W-FORM-231123/4
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	6.1	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in 10Web Form Builder Team Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder plugin <= 1.15.18 versions. **CVE ID : CVE-2023-45071**	N/A	A-10W-FORM-231123/5
Affected Version(s): * Up to (excluding) 1.15.20					
N/A	16-Oct-2023	9.8	The Form Maker by 10Web WordPress plugin before 1.15.20 does not validate signatures	N/A	A-10W-FORM-231123/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when creating them on the server from user input, allowing unauthenticated users to create arbitrary files and lead to RCE **CVE ID : CVE-2023-4666**		
Vendor: acfextended					
Product: advanced_custom_fields_extended					
Affected Version(s): * Up to (including) 0.8.9.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	The Advanced Custom Fields: Extended plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'acfe_form' shortcode in versions up to, and including, 0.8.9.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	https://plugins.trac.wordpress.org/changeset/2972880/acf-extended#file4	A-ACF-ADVA-231123/7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5292		
Vendor: add_shortcodes_actions_and_filters_project					
Product: add_shortcodes_actions_and_filters					
Affected Version(s): * Up to (including) 2.0.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Michael Simpson Add Shortcodes Actions And Filters plugin <= 2.0.9 versions. **CVE ID : CVE-2023-46072**	N/A	A-ADD-ADD_-231123/8
Vendor: admission_management_system_project					
Product: admission_management_system					
Affected Version(s): 1.0					
N/A	27-Oct-2023	8.8	A vulnerability was found in code-projects Admission Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file student_avatar.php. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier	N/A	A-ADM-ADMI-231123/9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability is VDB-243728. **CVE ID : CVE-2023-5829**		
Vendor: advanced_menu_widget_project					
Product: advanced_menu_widget					
Affected Version(s): * Up to (including) 0.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	The Advanced Menu Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'advMenu' shortcode in versions up to, and including, 0.4.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5085**	https://plugins.trac.wordpress.org/browser/advanced-menu-widget/trunk/class-advanced-menu-widget.php?rev=1471917#L74	A-ADV-ADVA-231123/10
Vendor: Advantech					
Product: r-seenet					
Affected Version(s): 2.4.23					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	9.8	Advantech R-SeeNet v2.4.23 allows an unauthenticated remote attacker to read from and write to the snmpmon.ini file, which contains sensitive information. **CVE ID : CVE-2023-5642**	https://tenable.com/security/research/tra-2023-33	A-ADV-R-SE-231123/11
Product: webaccess					
Affected Version(s): 9.1.3					
N/A	17-Oct-2023	7.5	Advantech WebAccess version 9.1.3 contains an exposure of sensitive information to an unauthorized actor vulnerability that could leak user credentials. **CVE ID : CVE-2023-4215**	N/A	A-ADV-WEBA-231123/12
Vendor: ad_inserter_project					
Product: ad_inserter					
Affected Version(s): * Up to (excluding) 2.7.31					
Missing Authorization	20-Oct-2023	7.5	The Ad Inserter for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 2.7.30 via the ai-debug-processing-fe URL parameter. This	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2969942%40ad-inserter%2Ftags%2F2.7.31&old=2922718%40ad-	A-AD_-AD_I-231123/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can allow unauthenticated attackers to extract sensitive data including installed plugins (present and active), active theme, various plugin settings, WordPress version, as well as some server settings such as memory limit, installation paths. **CVE ID : CVE-2023-4668**	inserter%2Ftrunk	
Vendor: alexanderlivanov					
Product: fotoscms2					
Affected Version(s): * Up to (including) 2.4.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Oct-2023	6.1	A vulnerability classified as problematic was found in AlexanderLivanov FotosCMS2 up to 2.4.3. This vulnerability affects unknown code of the file profile.php of the component Cookie Handler. The manipulation of the argument username leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may	N/A	A-ALE-FOTO-231123/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. VDB-243802 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-5837**		
Vendor: alexmacarthur					
Product: complete_open_graph					
Affected Version(s): * Up to (including) 3.4.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Alex MacArthur Complete Open Graph plugin <= 3.4.5 versions. **CVE ID : CVE-2023-45010**	N/A	A-ALE-COMP-231123/15
Vendor: alexraven					
Product: wp_report_post					
Affected Version(s): * Up to (including) 2.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Alex Raven WP Report Post plugin <= 2.1.2 versions. **CVE ID : CVE-2023-45769**	N/A	A-ALE-WP_R-231123/16
Vendor: Amazon					
Product: opensearch					
Affected Version(s): * Up to (excluding) 1.3.14.0					
Improper Preservation of	16-Oct-2023	5.4	OpenSearch is a community-driven, open source fork of Elasticsearch and	https://github.com/opensearch-project/security	A-AMA-OPEN-231123/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permissions			Kibana following the license change in early 2021. There is an issue with the implementation of tenant permissions in OpenSearch Dashboards where authenticated users with read-only access to a tenant can perform create, edit and delete operations on index metadata of dashboards and visualizations in that tenant, potentially rendering them unavailable. This issue does not affect index data, only metadata. Dashboards correctly enforces read-only permissions when indexing and updating documents. This issue does not provide additional read access to data users don't already have. This issue can be mitigated by disabling the tenants functionality for the cluster. Versions 1.3.14	/security/advisories/GHSA-72q2-gwwf-6hrv	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 2.11.0 contain a fix for this issue. **CVE ID : CVE-2023-45807**		
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.11.0.0					
Improper Preservation of Permissions	16-Oct-2023	5.4	OpenSearch is a community-driven, open source fork of Elasticsearch and Kibana following the license change in early 2021. There is an issue with the implementation of tenant permissions in OpenSearch Dashboards where authenticated users with read-only access to a tenant can perform create, edit and delete operations on index metadata of dashboards and visualizations in that tenant, potentially rendering them unavailable. This issue does not affect index data, only metadata. Dashboards correctly enforces read-only permissions when indexing and updating documents. This issue does not provide additional	https://github.com/opensearch-project/security/security/advisories/GHSA-72q2-gwwf-6hrv	A-AMA-OPEN-231123/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read access to data users don't already have. This issue can be mitigated by disabling the tenants functionality for the cluster. Versions 1.3.14 and 2.11.0 contain a fix for this issue. **CVE ID : CVE-2023-45807**		
Vendor: AMD					
Product: radeon_software					
Affected Version(s): * Up to (excluding) 23.9.2					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	A-AMD-RADE-231123/19
Affected Version(s): * Up to (excluding) 23.q4					
N/A	17-Oct-2023	7.8	An improper privilege	https://www.amd.com/en/cor	A-AMD-RADE-231123/20

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	porate/product-security/bulletin/AMD-SB-6009	
Vendor: amministrazione_trasparente_project					
Product: amministrazione_trasparente					
Affected Version(s): * Up to (including) 8.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Marco Milesi Amministrazione Trasparente plugin <= 8.0.2 versions. **CVE ID : CVE-2023-45758**	N/A	A-AMM-AMMI-231123/21
Vendor: anilankola					
Product: add_custom_body_class					
Affected Version(s): * Up to (including) 1.4.1					
Improper Neutralization of Input During Web Page Generation	21-Oct-2023	5.4	The Add Custom Body Class plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'add_custom_body_class' value in versions up to, and	N/A	A-ANI-ADD_-231123/22

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			including, 1.4.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5205**		
Vendor: anuragdeshmukh					
Product: cpt_shortcode_generator					
Affected Version(s): * Up to (including) 1.0					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Anurag Deshmukh CPT Shortcode Generator plugin <= 1.0 versions. **CVE ID : CVE-2023-45643**	N/A	A-ANU-CPT_-231123/23
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Anurag Deshmukh CPT Shortcode Generator plugin <= 1.0 versions. **CVE ID : CVE-2023-45644**	N/A	A-ANU-CPT_-231123/24
Vendor: Apache					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: airflow					
Affected Version(s): From (including) 1.10.0 Up to (excluding) 2.7.0					
Insertion of Sensitive Information into Log File	28-Oct-2023	7.5	Insertion of Sensitive Information into Log File vulnerability in Apache Airflow Celery provider, Apache Airflow. Sensitive information logged as clear text when rediss, amqp, rpc protocols are used as Celery result backend Note: the vulnerability is about the information exposed in the logs not about accessing the logs. This issue affects Apache Airflow Celery provider: from 3.3.0 through 3.4.0; Apache Airflow: from 1.10.0 through 2.6.3. Users are recommended to upgrade Airflow Celery provider to version 3.4.1 and Apache Airlfow to version 2.7.0 which fixes the issue.	https://github.com/apache/airflow/pull/34954, https://lists.apache.org/thread/wm1jfmks7r6m7bj0mq4lmw3998svn46n	A-APA-AIRF-231123/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46215		
Affected Version(s): From (including) 2.4.0 Up to (excluding) 2.7.0					
N/A	23-Oct-2023	4.3	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Airflow.This issue affects Apache Airflow from 2.4.0 to 2.7.0. Sensitive configuration information has been exposed to authenticated users with the ability to read configuration via Airflow REST API for configuration even when the expose_config option is set to non-sensitive-only. The expose_config option is False by default. It is recommended to upgrade to a version that is not affected if you set expose_config to non-sensitive-only configuration. This is a different error than CVE-2023-45348 which allows authenticated user to retrieve	https://github.com/apache/airflow/pull/32261, https://lists.apache.org/thread/yw4vzm0c5lqkwm0bxv6qy03yfd1od4nw	A-APA-AIRF-231123/26

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			individual configuration values in 2.7.* by specially crafting their request (solved in 2.7.2). Users are recommended to upgrade to version 2.7.2, which fixes the issue and additionally fixes CVE-2023-45348. **CVE ID : CVE-2023-46288**		
Product: airflow_celery_provider					
Affected Version(s): From (including) 3.3.0 Up to (including) 3.4.0					
Insertion of Sensitive Information into Log File	28-Oct-2023	7.5	Insertion of Sensitive Information into Log File vulnerability in Apache Airflow Celery provider, Apache Airflow. Sensitive information logged as clear text when rediss, amqp, rpc protocols are used as Celery result backend Note: the vulnerability is about the information exposed in the logs not about accessing the logs.	https://github.com/apache/airflow/pull/34954, https://lists.apache.org/thread/wm1jfmks7r6m7bj0mq4lmw3998svn46n	A-APA-AIRF-231123/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Apache Airflow Celery provider: from 3.3.0 through 3.4.0; Apache Airflow: from 1.10.0 through 2.6.3. Users are recommended to upgrade Airflow Celery provider to version 3.4.1 and Apache Airlfow to version 2.7.0 which fixes the issue. **CVE ID : CVE-2023-46215**		
Product: brpc					
Affected Version(s): * Up to (excluding) 1.6.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-2023	6.1	Security vulnerability in Apache bRPC <=1.6.0 on all platforms allows attackers to inject XSS code to the builtin rpcz page. An attacker that can send http request to bRPC server with rpcz enabled can inject arbitrary XSS code to the builtin rpcz page. Solution (choose one of three): 1. upgrade to bRPC > 1.6.0, download link:	https://lists.apache.org/thread/6syxv32fqgl30brfpttrk4rfsb983hl4	A-APA-BRPC-231123/28

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			https://dist.apache.org/repos/dist/release/brpc/1.6.1/ 2. If you are using an old version of bRPC and hard to upgrade, you can apply this patch: https://github.com/apache/brpc/pull/2411 3. disable rpcz feature **CVE ID : CVE-2023-45757**		
Product: http_server					
Affected Version(s): * Up to (excluding) 2.4.58					
Uncontrolled Resource Consumption	23-Oct-2023	5.9	When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the	https://httpd.apache.org/security/vulnerabilities_24.html	A-APA-HTTP-231123/29

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue. **CVE ID : CVE-2023-45802**		
Affected Version(s): * Up to (including) 2.4.57					
Out-of-bounds Read	23-Oct-2023	7.5	Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57. **CVE ID : CVE-2023-31122**	https://httpd.apache.org/security/vulnerabilities_24.html	A-APA-HTTP-231123/30
Affected Version(s): From (including) 2.4.55 Up to (excluding) 2.4.58					
Uncontrolled	23-Oct-2023	7.5	An attacker, opening a HTTP/2	https://httpd.apache.org/secur	A-APA-HTTP-231123/31

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			connection with an initial window size of 0, was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well known "slow loris" attack pattern. This has been fixed in version 2.4.58, so that such connection are terminated properly after the configured connection timeout. This issue affects Apache HTTP Server: from 2.4.55 through 2.4.57. Users are recommended to upgrade to version 2.4.58, which fixes the issue. **CVE ID : CVE-2023-43622**	ity/vulnerabilities_24.html	
Product: inlong					
Affected Version(s): From (including) 1.4.0 Up to (excluding) 1.9.0					
Deserialization of Untrusted Data	19-Oct-2023	7.5	Deserialization of Untrusted Data Vulnerability in Apache Software	N/A	A-APA-INLO-231123/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Foundation Apache InLong. This issue affects Apache InLong: from 1.4.0 through 1.8.0, the attacker can use \t to bypass. Users are advised to upgrade to Apache InLong's 1.9.0 or cherry-pick [1] to solve it. [1] https://github.com/apache/inlong/pull/8814 **CVE ID : CVE-2023-46227**		
Affected Version(s): From (including) 1.4.0 Up to (including) 1.8.0					
Authorization Bypass Through User-Controlled Key	16-Oct-2023	9.8	Authorization Bypass Through User-Controlled Key vulnerability in Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.8.0, some sensitive params checks will be bypassed, like "autoDeserizalize", "allowLoadLocalInfile"..... Users are advised to upgrade to Apache InLong's 1.9.0 or cherry-pick [1] to solve it.	https://lists.apache.org/thread/16gtk7rpdm1rof075ro83fkrnhbzn5sh	A-APA-INLO-231123/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[1] https://github.com/apache/inlong/pull/8604 **CVE ID : CVE-2023-43668**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Oct-2023	7.5	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.8.0, the attacker can create misleading or false records, making it harder to audit and trace malicious activities. Users are advised to upgrade to Apache InLong's 1.8.0 or cherry-pick [1] to solve it. [1] https://github.com/apache/inlong/pull/8628 **CVE ID : CVE-2023-43667**	N/A	A-APA-INLO-231123/34
Insufficient Verification of Data Authenticity	16-Oct-2023	6.5	Insufficient Verification of Data Authenticity vulnerability in Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.8.0,	https://lists.apache.org/thread/scbgh3ty3xcxm3q33r2t9f42gwwo1why	A-APA-INLO-231123/35

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			General user can view all user data like Admin account. Users are advised to upgrade to Apache InLong's 1.9.0 or cherry-pick [1] to solve it. [1] https://github.com/apache/inlong/pull/8623 **CVE ID : CVE-2023-43666**		
Product: santuario_xml_security_for_java					
Affected Version(s): * Up to (excluding) 2.2.6					
Insertion of Sensitive Information into Log File	20-Oct-2023	6.5	All versions of Apache Santuario - XML Security for Java prior to 2.2.6, 2.3.4, and 3.0.3, when using the JSR 105 API, are vulnerable to an issue where a private key may be disclosed in log files when generating an XML Signature and logging with debug level is enabled. Users are recommended to upgrade to version 2.2.6, 2.3.4, or 3.0.3, which fixes this issue. **CVE ID : CVE-2023-44483**	https://lists.apache.org/thread/vmqbp9mfxtrf0kmbnnmbn3h9j6dr9q55	A-APA-SANT-231123/36
Affected Version(s): From (including) 2.3.0 Up to (excluding) 2.3.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	20-Oct-2023	6.5	All versions of Apache Santuario - XML Security for Java prior to 2.2.6, 2.3.4, and 3.0.3, when using the JSR 105 API, are vulnerable to an issue where a private key may be disclosed in log files when generating an XML Signature and logging with debug level is enabled. Users are recommended to upgrade to version 2.2.6, 2.3.4, or 3.0.3, which fixes this issue. **CVE ID : CVE-2023-44483**	https://lists.apache.org/thread/vmqbp9mfxtrf0kmbnnmbn3h9j6dr9q55	A-APA-SANT-231123/37
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.3					
Insertion of Sensitive Information into Log File	20-Oct-2023	6.5	All versions of Apache Santuario - XML Security for Java prior to 2.2.6, 2.3.4, and 3.0.3, when using the JSR 105 API, are vulnerable to an issue where a private key may be disclosed in log files when generating an XML Signature and logging with debug level is enabled. Users are recommended to	https://lists.apache.org/thread/vmqbp9mfxtrf0kmbnnmbn3h9j6dr9q55	A-APA-SANT-231123/38

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade to version 2.2.6, 2.3.4, or 3.0.3, which fixes this issue. **CVE ID : CVE-2023-44483**		
Product: shenyu					
Affected Version(s): 2.5.1					
Server-Side Request Forgery (SSRF)	19-Oct-2023	6.5	There exists an SSRF (Server-Side Request Forgery) vulnerability located at the /sandbox/proxyGateway endpoint. This vulnerability allows us to manipulate arbitrary requests and retrieve corresponding responses by inputting any URL into the requestUrl parameter. Of particular concern is our ability to exert control over the HTTP method, cookies, IP address, and headers. This effectively grants us the capability to dispatch complete HTTP requests to hosts of our choosing. This issue affects Apache ShenYu: 2.5.1.	https://lists.apache.org/thread/chprswxvb22z35vnoxv9tt3zksnm977d	A-APA-SHEN-231123/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Upgrade to Apache ShenYu 2.6.0 or apply patch https://github.com/apache/shenyu/pull/4776 . **CVE ID : CVE-2023-25753**		
Product: traffic_server					
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.1.9					
Exposure of Sensitive Information to an Unauthorized Actor	17-Oct-2023	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Traffic Server.This issue affects Apache Traffic Server: from 8.0.0 through 8.1.8, from 9.0.0 through 9.2.2. Users are recommended to upgrade to version 8.1.9 or 9.2.3, which fixes the issue. **CVE ID : CVE-2023-41752**	https://lists.apache.org/thread/5py8h42mxfsn8l1wy6o41xwhsjlsd87q	A-APA-TRAF-231123/40
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.2.3					
Improper Input Validation	17-Oct-2023	7.5	Improper Input Validation vulnerability in Apache Traffic Server with malformed HTTP/2 frames.This issue affects Apache Traffic Server:	https://lists.apache.org/thread/5py8h42mxfsn8l1wy6o41xwhsjlsd87q	A-APA-TRAF-231123/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from 9.0.0 through 9.2.2. Users are recommended to upgrade to version 9.2.3, which fixes the issue. **CVE ID : CVE-2023-39456**		
Exposure of Sensitive Information to an Unauthorized Actor	17-Oct-2023	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Traffic Server.This issue affects Apache Traffic Server: from 8.0.0 through 8.1.8, from 9.0.0 through 9.2.2. Users are recommended to upgrade to version 8.1.9 or 9.2.3, which fixes the issue. **CVE ID : CVE-2023-41752**	https://lists.apache.org/thread/5py8h42mxfsn8l1wy6o41xwhsjlsd87q	A-APA-TRAF-231123/42
Vendor: apointzilla					
Product: appointment_calendar					
Affected Version(s): * Up to (including) 2.9.6					
Cross-Site Request Forgery (CSRF)	25-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Scientech It Solution Appointment Calendar plugin <= 2.9.6 versions.	N/A	A-APO-APPO-231123/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46198		
Vendor: apollographql					
Product: apollo_helms-charts_router					
Affected Version(s): From (including) 1.31.0 Up to (including) 1.32.0					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2023	7.5	The Apollo Router is a configurable, high-performance graph router written in Rust to run a federated supergraph that uses Apollo Federation. Affected versions are subject to a Denial-of-Service (DoS) type vulnerability which causes the Router to panic and terminate when a multi-part response is sent. When users send queries to the router that uses the `@defer` or Subscriptions, the Router will panic. To be vulnerable, users of Router must have a coprocessor with `coprocessor.supergraph.response` configured in their `router.yaml` and also to support either `@defer` or Subscriptions. Apollo Router version 1.33.0 has	https://github.com/apollographql/router/security/advisories/GHSA-r344-xw3p-2frj, https://github.com/apollographql/router/pull/4014	A-APO-APOL-231123/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a fix for this vulnerability which was introduced in PR #4014. Users are advised to upgrade. Users unable to upgrade should avoid using the coprocessor supergraph response or disable defer and subscriptions support and continue to use the coprocessor supergraph response. **CVE ID : CVE-2023-45812**		
Product: apollo_router					
Affected Version(s): From (including) 1.31.0 Up to (including) 1.32.0					
Improper Check for Unusual or Exceptional Conditions	18-Oct-2023	7.5	The Apollo Router is a configurable, high-performance graph router written in Rust to run a federated supergraph that uses Apollo Federation. Affected versions are subject to a Denial-of-Service (DoS) type vulnerability which causes the Router to panic and terminate when a multi-part response is sent. When users send queries to the	https://github.com/apollographql/router/security/advisories/GHSA-r344-xw3p-2frj, https://github.com/apollographql/router/pull/4014	A-APO-APOL-231123/45

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			router that uses the `@defer` or Subscriptions, the Router will panic. To be vulnerable, users of Router must have a coprocessor with `coprocessor.supergraph.response` configured in their `router.yaml` and also to support either `@defer` or Subscriptions. Apollo Router version 1.33.0 has a fix for this vulnerability which was introduced in PR #4014. Users are advised to upgrade. Users unable to upgrade should avoid using the coprocessor supergraph response or disable defer and subscriptions support and continue to use the coprocessor supergraph response. **CVE ID : CVE-2023-45812**		
Vendor: appjetty					
Product: copy_or_move_comments					
Affected Version(s): * Up to (including) 5.0.4					
Improper Neutralizat	25-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting	N/A	A-APP-COPY-231123/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			(XSS) vulnerability in Biztechc Copy or Move Comments plugin <= 5.0.4 versions. **CVE ID : CVE-2023-45634**		
Vendor: Apple					
Product: safari					
Affected Version(s): * Up to (excluding) 17.1					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2023-40447**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	A-APP-SAFA-231123/47
Use After Free	25-Oct-2023	8.8	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-	A-APP-SAFA-231123/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			content may lead to arbitrary code execution. **CVE ID : CVE-2023-41976**	us/HT213987, https://support.apple.com/en-us/HT213984	
N/A	25-Oct-2023	8.8	A logic issue was addressed with improved checks. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2023-42852**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	A-APP-SAFA-231123/49
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, Safari 17.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Processing web content may lead to a denial-of-service. **CVE ID : CVE-2023-41983**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213984	A-APP-SAFA-231123/50
Vendor: archerirm					
Product: archer					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 6.0 Up to (excluding) 6.13.0.2.2					
Exposure of Resource to Wrong Sphere	17-Oct-2023	6.5	Archer Platform 6.x before 6.13 P2 HF2 (6.13.0.2.2) contains a sensitive information disclosure vulnerability. An authenticated attacker could potentially obtain access to sensitive information via a popup warning message. 6.14 (6.14.0) is also a fixed release. **CVE ID : CVE-2023-45357**	https://www.archerirm.community/t5/platform-announcements/archer-update-for-multiple-vulnerabilities/ta-p/708617	A-ARC-ARCH-231123/51
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	5.4	Archer Platform 6.x before 6.13 P2 HF2 (6.13.0.2.2) contains a stored cross-site scripting (XSS) vulnerability. A remote authenticated malicious Archer user could potentially exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. When victim users access the data store through their browsers, the malicious code gets executed by the web browser in the context of the	https://www.archerirm.community/t5/platform-announcements/archer-update-for-multiple-vulnerabilities/ta-p/708617	A-ARC-ARCH-231123/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable application. 6.14 (6.14.0) is also a fixed release. **CVE ID : CVE-2023-45358**		
Vendor: archivebox					
Product: archivebox					
Affected Version(s): * Up to (including) 0.6.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2023	5.4	ArchiveBox is an open source self-hosted web archiving system. Any users who are using the `wget` extractor and view the content it outputs. The impact is potentially severe if you are logged in to the ArchiveBox admin site in the same browser session and view an archived malicious page designed to target your ArchiveBox instance. Malicious Javascript could potentially act using your logged-in admin credentials and add/remove/modify snapshots, add/remove/modify ArchiveBox users, and generally do anything an admin user could do. The	https://github.com/ArchiveBox/ArchiveBox/security/advisories/GHSA-cr45-98w9-gwqx	A-ARC-ARCH-231123/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impact is less severe for non-logged-in users, as malicious Javascript cannot *modify* any archives, but it can still *read* all the other archived content by fetching the snapshot index and iterating through it. Because all of ArchiveBox's archived content is served from the same host and port as the admin panel, when archived pages are viewed the JS executes in the same context as all the other archived pages (and the admin panel), defeating most of the browser's usual CORS/CSRF security protections and leading to this issue. A patch is being developed in https://github.com/ArchiveBox/ArchiveBox/issues/239. As a mitigation for this issue would be to disable the wget extractor by setting `archivebox config --set SAVE_WGET=False		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`, ensure you are always logged out, or serve only a [static HTML version](https://github.com/ArchiveBox/ArchiveBox/wiki/Publishing-Your-Archive#2-export-and-host-it-as-static-html) of your archive. **CVE ID : CVE-2023-45815**		
Vendor: arduino					
Product: create_agent					
Affected Version(s): * Up to (excluding) 1.3.3					
Insufficient Verification of Data Authenticity	18-Oct-2023	7.8	Arduino Create Agent is a package to help manage Arduino development. The vulnerability affects the endpoint `/v2/pkgs/tools/installed`. A user who has the ability to perform HTTP requests to the localhost interface, or is able to bypass the CORS configuration, can escalate his privileges to those of the user running the Arduino Create Agent service via a crafted HTTP POST request. This issue has been	https://github.com/arduino/arduino-create-agent/security/advisories/GHSA-4x5q-q7wc-q22p	A-ARD-CREA-231123/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addressed in version `1.3.3`. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-43800**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-2023	7.8	Arduino Create Agent is a package to help manage Arduino development. This vulnerability affects the endpoint `/upload` which handles request with the `filename` parameter. A user who has the ability to perform HTTP requests to the localhost interface, or is able to bypass the CORS configuration, can escalate their privileges to those of the user running the Arduino Create Agent service via a crafted HTTP POST request. This issue has been addressed in version `1.3.3`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	https://github.com/arduino/arduino-create-agent/security/advisories/GHSA-75j7-w798-cwwx	A-ARD-CREA-231123/55

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43802		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-2023	7.1	Arduino Create Agent is a package to help manage Arduino development. This vulnerability affects the endpoint `/v2/pkgs/tools/installed` and the way it handles plugin names supplied as user input. A user who has the ability to perform HTTP requests to the localhost interface, or is able to bypass the CORS configuration, can delete arbitrary files or folders belonging to the user that runs the Arduino Create Agent via a crafted HTTP DELETE request. This issue has been addressed in version `1.3.3`. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-43801**	https://github.com/arduino/arduino-create-agent/security/advisories/GHSA-mjq6-pv9c-qppq	A-ARD-CREA-231123/56
Improper Limitation	18-Oct-2023	7.1	Arduino Create Agent is a package	https://github.com/arduino/ar	A-ARD-CREA-231123/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			to help manage Arduino development. This vulnerability affects the endpoint `/v2/pkgs/tools/installed` and the way it handles plugin names supplied as user input. A user who has the ability to perform HTTP requests to the localhost interface, or is able to bypass the CORS configuration, can delete arbitrary files or folders belonging to the user that runs the Arduino Create Agent via a crafted HTTP POST request. This issue has been addressed in version `1.3.3`. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-43803**	duino-create-agent/security/advisories/GHSA-m5jc-r4gf-c6p8	
Vendor: armemberplugin					
Product: armember					
Affected Version(s): * Up to (including) 4.0.14					
Improper Neutralizat	20-Oct-2023	4.8	The ARMember Lite - Membership	https://plugins.trac.wordpress.	A-ARM-ARME-231123/58

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 4.0.14 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-3996**	org/changeset?sfp_email=&sfph_mail=&reponame=&new=2905086%40armember-membership%2Ftrunk&old=2885708%40armember-membership%2Ftrunk&sfp_email=&sfph_mail=	
Vendor: arrowplugins					
Product: social_feed					
Affected Version(s): * Up to (including) 2.2.0					
Improper Neutralization of Input During Web Page Generation	17-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Arrow Plugins Social Feed | Custom Feed for Social Media	N/A	A-ARR-SOCI-231123/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Networks plugin <= 2.2.0 versions. **CVE ID : CVE-2023-45003**		
Product: the_awesome_feed					
Affected Version(s): * Up to (including) 2.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Arrow Plugins The Awesome Feed – Custom Feed plugin <= 2.2.5 versions. **CVE ID : CVE-2023-46077**	N/A	A-ARR-THE_-231123/60
Vendor: artifacthub					
Product: hub					
Affected Version(s): * Up to (excluding) 1.16.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Oct-2023	7.5	Artifact Hub is a web-based application that enables finding, installing, and publishing packages and configurations for CNCF projects. During a security audit of Artifact Hub's code base a security researcher identified a bug in which by using symbolic links in certain kinds of repositories loaded into Artifact Hub, it was possible to read internal files. Artifact Hub	N/A	A-ART-HUB-231123/61

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			indexes content from a variety of sources, including git repositories. When processing git based repositories, Artifact Hub clones the repository and, depending on the artifact kind, reads some files from it. During this process, in some cases, no validation was done to check if the file was a symbolic link. This made possible to read arbitrary files in the system, potentially leaking sensitive information. This issue has been resolved in version `1.16.0`. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45823**		
N/A	19-Oct-2023	6.3	Artifact Hub is a web-based application that enables finding, installing, and publishing packages and configurations for CNCF projects.	N/A	A-ART-HUB-231123/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			During a security audit of Artifact Hub's code base a security researcher identified a bug in which the `registryIsDockerHub` function was only checking that the registry domain had the `docker.io` suffix. Artifact Hub allows providing some Docker credentials that are used to increase the rate limit applied when interacting with the Docker Hub registry API to read publicly available content. Due to the incorrect check described above, it'd be possible to hijack those credentials by purchasing a domain which ends with `docker.io` and deploying a fake OCI registry on it. <https://artifacthub.io/> uses some credentials that only have permissions to read public content available in the Docker Hub. However, even though credentials		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for private repositories (disabled on `artifacthub.io`) are handled in a different way, other Artifact Hub deployments could have been using them for a different purpose. This issue has been resolved in version `1.16.0`. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45821**		
Server-Side Request Forgery (SSRF)	19-Oct-2023	5.3	Artifact Hub is a web-based application that enables finding, installing, and publishing packages and configurations for CNCF projects. During a security audit of Artifact Hub's code base a security researcher identified a bug in which a default unsafe rego built-in was allowed to be used when defining authorization policies. Artifact Hub includes a fine-grained authorization	N/A	A-ART-HUB-231123/63

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mechanism that allows organizations to define what actions can be performed by their members. It is based on customizable authorization policies that are enforced by the `Open Policy Agent`. Policies are written using `rego` and their data files are expected to be json documents. By default, `rego` allows policies to make HTTP requests, which can be abused to send requests to internal resources and forward the responses to an external entity. In the context of Artifact Hub, this capability should have been disabled. This issue has been resolved in version `1.16.0`. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45822**		
Vendor: Artifex					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: jbig2dec					
Affected Version(s): 0.20					
N/A	31-Oct-2023	6.5	Artifex Software jbig2dec v0.20 was discovered to contain a SEGV vulnerability via jbig2_error at /jbig2dec/jbig2.c. **CVE ID : CVE-2023-46361**	N/A	A-ART-JBIG-231123/64
Product: mupdf					
Affected Version(s): 1.21.1					
Uncontrolled Recursion	31-Oct-2023	5.5	MuPDF v1.21.1 was discovered to contain an infinite recursion in the component pdf_mark_list_push . This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted PDF file. **CVE ID : CVE-2023-31794**	N/A	A-ART-MUPD-231123/65
Vendor: Arubanetworks					
Product: airwave					
Affected Version(s): * Up to (including) 8.2.15.2					
N/A	17-Oct-2023	6.5	A vulnerability exists which allows an authenticated attacker to access sensitive information on the AirWave Management Platform web-based management interface.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-015.txt	A-ARU-AIRW-231123/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation allows the attacker to gain access to some data that could be further exploited to laterally access devices managed and monitored by the AirWave server. **CVE ID : CVE-2023-4896**		
Affected Version(s): From (including) 8.3.0 Up to (excluding) 8.3.0.2					
N/A	17-Oct-2023	6.5	A vulnerability exists which allows an authenticated attacker to access sensitive information on the AirWave Management Platform web-based management interface. Successful exploitation allows the attacker to gain access to some data that could be further exploited to laterally access devices managed and monitored by the AirWave server. **CVE ID : CVE-2023-4896**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-015.txt	A-ARU-AIRW-231123/67
Product: clearpass_policy_manager					
Affected Version(s): * Up to (excluding) 6.9.13					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	8.8	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could exploit this vulnerability to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster. **CVE ID : CVE-2023-43507**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/68
N/A	25-Oct-2023	7.8	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/69

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on the Linux instance. **CVE ID : CVE-2023-43506**		
Incorrect Authorization	25-Oct-2023	6.5	Vulnerabilities in the web-based management interface of ClearPass Policy Manager allow an attacker with read-only privileges to perform actions that change the state of the ClearPass Policy Manager instance. Successful exploitation of these vulnerabilities allow an attacker to complete state-changing actions in the web-based management interface that should not be allowed by their current level of authorization on the platform. **CVE ID : CVE-2023-43508**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/70
Improper Neutralization of Special Elements used in a Command ('Comman	25-Oct-2023	6.3	A vulnerability in the ClearPass Policy Manager web-based management interface allows remote authenticated	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/71

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as a non-privileged user on the underlying operating system leading to partial system compromise. **CVE ID : CVE-2023-43510**		
N/A	25-Oct-2023	5.8	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to send notifications to computers that are running ClearPass OnGuard. These notifications can then be used to phish users or trick them into downloading malicious software. **CVE ID : CVE-2023-43509**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/72
Affected Version(s): 6.10.8					
Improper Neutralizat	25-Oct-2023	8.8	A vulnerability in the web-based	https://www.arubanetworks.co	A-ARU-CLEA-231123/73

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			management interface of ClearPass Policy Manager could allow an authenticated remo te attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could exploit this vulnerability to obtain and modify sensitive informati on in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster. **CVE ID : CVE-2023-43507**	m/assets/alert/ ARUBA-PSA-2023-016.txt	
N/A	25-Oct-2023	7.8	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level privileges on the Linux instance.	https://www.ar ubanetworks.co m/assets/alert/ ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/74

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43506		
Incorrect Authorization	25-Oct-2023	6.5	Vulnerabilities in the web-based management interface of ClearPass Policy Manager allow an attacker with read-only privileges to perform actions that change the state of the ClearPass Policy Manager instance. Successful exploitation of these vulnerabilities allow an attacker to complete state-changing actions in the web-based management interface that should not be allowed by their current level of authorization on the platform. **CVE ID : CVE-2023-43508**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/75
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	6.3	A vulnerability in the ClearPass Policy Manager web-based management interface allows remote authenticated users to run arbitrary	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/76

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as a non-privileged user on the underlying operating system leading to partial system compromise. **CVE ID : CVE-2023-43510**		
N/A	25-Oct-2023	5.8	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to send notifications to computers that are running ClearPass OnGuard. These notifications can then be used to phish users or trick them into downloading malicious software. **CVE ID : CVE-2023-43509**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/77
Affected Version(s): 6.9.13					
Improper Neutralization of Special	25-Oct-2023	8.8	A vulnerability in the web-based management interface	https://www.arubanetworks.com/assets/alert/	A-ARU-CLEA-231123/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			of ClearPass Policy Manager could allow an authenticated remo te attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could exploit this vulnerability to obtain and modify sensitive informati on in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster. **CVE ID : CVE-2023-43507**	ARUBA-PSA-2023-016.txt	
N/A	25-Oct-2023	7.8	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level privileges on the Linux instance. **CVE ID : CVE-2023-43506**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	25-Oct-2023	6.5	Vulnerabilities in the web-based management interface of ClearPass Policy Manager allow an attacker with read-only privileges to perform actions that change the state of the ClearPass Policy Manager instance. Successful exploitation of these vulnerabilities allow an attacker to complete state-changing actions in the web-based management interface that should not be allowed by their current level of authorization on the platform. **CVE ID : CVE-2023-43508**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/80
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	6.3	A vulnerability in the ClearPass Policy Manager web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow an attacker to execute arbitrary commands as a non-privileged user on the underlying operating system leading to partial system compromise. **CVE ID : CVE-2023-43510**		
N/A	25-Oct-2023	5.8	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to send notifications to computers that are running ClearPass OnGuard. These notifications can then be used to phish users or trick them into downloading malicious software. **CVE ID : CVE-2023-43509**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/82
Affected Version(s): From (including) 6.10.0 Up to (excluding) 6.10.8					
Improper Neutralization of Special Elements used in an	25-Oct-2023	8.8	A vulnerability in the web-based management interface of ClearPass Policy Manager could	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/83

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could exploit this vulnerability to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster. **CVE ID : CVE-2023-43507**		
N/A	25-Oct-2023	7.8	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level privileges on the Linux instance. **CVE ID : CVE-2023-43506**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/84

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	25-Oct-2023	6.5	Vulnerabilities in the web-based management interface of ClearPass Policy Manager allow an attacker with read-only privileges to perform actions that change the state of the ClearPass Policy Manager instance. Successful exploitation of these vulnerabilities allow an attacker to complete state-changing actions in the web-based management interface that should not be allowed by their current level of authorization on the platform. **CVE ID : CVE-2023-43508**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/85
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	6.3	A vulnerability in the ClearPass Policy Manager web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow an attacker to execute arbitrary commands as a non-privileged user on the underlying operating system leading to partial system compromise. **CVE ID : CVE-2023-43510**		
N/A	25-Oct-2023	5.8	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to send notifications to computers that are running ClearPass OnGuard. These notifications can then be used to phish users or trick them into downloading malicious software. **CVE ID : CVE-2023-43509**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/87
Affected Version(s): From (including) 6.11.0 Up to (including) 6.11.4					
Improper Neutralization of Special Elements used in an	25-Oct-2023	8.8	A vulnerability in the web-based management interface of ClearPass Policy Manager could	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could exploit this vulnerability to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster. **CVE ID : CVE-2023-43507**		
N/A	25-Oct-2023	7.8	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level privileges on the Linux instance. **CVE ID : CVE-2023-43506**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/89

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	25-Oct-2023	6.5	Vulnerabilities in the web-based management interface of ClearPass Policy Manager allow an attacker with read-only privileges to perform actions that change the state of the ClearPass Policy Manager instance. Successful exploitation of these vulnerabilities allow an attacker to complete state-changing actions in the web-based management interface that should not be allowed by their current level of authorization on the platform. **CVE ID : CVE-2023-43508**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/90
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	6.3	A vulnerability in the ClearPass Policy Manager web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow an attacker to execute arbitrary commands as a non-privileged user on the underlying operating system leading to partial system compromise. **CVE ID : CVE-2023-43510**		
N/A	25-Oct-2023	5.8	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to send notifications to computers that are running ClearPass OnGuard. These notifications can then be used to phish users or trick them into downloading malicious software. **CVE ID : CVE-2023-43509**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	A-ARU-CLEA-231123/92
Vendor: ashlar					
Product: argon					
Affected Version(s): * Up to (including) 12					
Out-of-bounds Write	26-Oct-2023	7.8	In Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share	N/A	A-ASH-ARGO-231123/93

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v12 SP0 Build (1204.77), the affected applications lack proper validation of user-supplied data when parsing XE files. This could lead to an out-of-bounds write. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-39427**		
Product: cobalt					
Affected Version(s): * Up to (including) 12					
Out-of-bounds Write	26-Oct-2023	7.8	In Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share v12 SP0 Build (1204.77), the affected applications lack proper validation of user-supplied data when parsing XE files. This could lead to an out-of-bounds write. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process.	N/A	A-ASH-COBA-231123/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39427		
Product: graphite					
Affected Version(s): * Up to (including) 13.0.48					
Out-of-bounds Write	26-Oct-2023	7.8	In Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share v12 SP0 Build (1204.77), the affected applications lack proper validation of user-supplied data when parsing XE files. This could lead to an out-of-bounds write. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-39427**	N/A	A-ASH-GRAP-231123/95
Out-of-bounds Read	26-Oct-2023	7.8	In Ashlar-Vellum Graphite v13.0.48, the affected application lacks proper validation of user-supplied data when parsing VC6 files. This could lead to an out-of-bounds read. An attacker could leverage this vulnerability to execute arbitrary	N/A	A-ASH-GRAP-231123/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the current process. **CVE ID : CVE-2023-39936**		
Product: lithium					
Affected Version(s): * Up to (including) 12					
Out-of-bounds Write	26-Oct-2023	7.8	In Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share v12 SP0 Build (1204.77), the affected applications lack proper validation of user-supplied data when parsing XE files. This could lead to an out-of-bounds write. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-39427**	N/A	A-ASH-LITH-231123/97
Product: xenon					
Affected Version(s): * Up to (including) 12					
Out-of-bounds Write	26-Oct-2023	7.8	In Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share v12 SP0 Build (1204.77), the affected	N/A	A-ASH-XENO-231123/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applications lack proper validation of user-supplied data when parsing XE files. This could lead to an out-of-bounds write. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-39427**		
Vendor: Automattic					
Product: activitypub					
Affected Version(s): * Up to (excluding) 1.0.0					
N/A	16-Oct-2023	5.4	The ActivityPub WordPress plugin before 1.0.0 does not sanitize and escape some data from post content, which could allow contributor and above role to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-3746**	N/A	A-AUT-ACTI-231123/99
N/A	16-Oct-2023	5.4	The ActivityPub WordPress plugin before 1.0.0 does not escape user metadata before outputting them in mentions, which could allow users with a role of	N/A	A-AUT-ACTI-231123/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Contributor and above to perform Stored XSS attacks **CVE ID : CVE-2023-5057**		
N/A	16-Oct-2023	4.3	The ActivityPub WordPress plugin before 1.0.0 does not ensure that post titles to be displayed are public and belong to the plugin, allowing any authenticated user, such as subscriber to retrieve the title of arbitrary post (such as draft and private) via an IDOR vector **CVE ID : CVE-2023-3706**	N/A	A-AUT-ACTI-231123/101
N/A	16-Oct-2023	4.3	The ActivityPub WordPress plugin before 1.0.0 does not ensure that post contents to be displayed are public and belong to the plugin, allowing any authenticated user, such as subscriber to retrieve the content of arbitrary post (such as draft and private) via an IDOR vector. Password protected posts are	N/A	A-AUT-ACTI-231123/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not affected by this issue. **CVE ID : CVE-2023-3707**		
Vendor: auto_login_new_user_after_registration_project					
Product: auto_login_new_user_after_registration					
Affected Version(s): * Up to (including) 1.9.6					
Cross-Site Request Forgery (CSRF)	25-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Jeff Sherk Auto Login New User After Registration plugin <= 1.9.6 versions. **CVE ID : CVE-2023-46202**	N/A	A-AUT-AUTO-231123/103
Vendor: awesometogi					
Product: product-category-tree					
Affected Version(s): * Up to (including) 2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in AWESOME TOGI Product Category Tree plugin <= 2.5 versions. **CVE ID : CVE-2023-45054**	N/A	A-AWE-PROD-231123/104
Product: product_category_tree					
Affected Version(s): * Up to (including) 2.5					
Cross-Site Request Forgery (CSRF)	25-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in AWESOME TOGI Product Category Tree plugin <= 2.5 versions.	N/A	A-AWE-PROD-231123/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46151		
Vendor: awsm					
Product: job_openings					
Affected Version(s): * Up to (excluding) 3.4.3					
Exposure of Resource to Wrong Sphere	16-Oct-2023	5.3	The WP Job Openings WordPress plugin before 3.4.3 does not block listing the contents of the directories where it stores attachments to job applications, allowing unauthenticated visitors to list and download private attachments if the autoindex feature of the web server is enabled. **CVE ID : CVE-2023-4933**	N/A	A-AWS-JOB_-231123/106
Vendor: bala-krishna					
Product: category_seo_meta_tags					
Affected Version(s): * Up to (including) 2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Bala Krishna, Sergey Yakovlev Category SEO Meta Tags plugin <= 2.5 versions. **CVE ID : CVE-2023-46091**	N/A	A-BAL-CATE-231123/107
Vendor: Bannersky					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: bsk_pdf_manager					
Affected Version(s): * Up to (including) 3.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	The BSK PDF Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'bsk-pdfm-category-dropdown' shortcode in versions up to, and including, 3.4.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5110**	https://plugins.trac.wordpress.org/browser/bsk-pdf-manager/trunk/classes/shortcodes/category/category-dropdown.php?rev=2885460#L36	A-BAN-BSK_-231123/108
Vendor: Basercms					
Product: basercms					
Affected Version(s): * Up to (excluding) 4.8.0					
Cross-Site Request Forgery (CSRF)	30-Oct-2023	9.8	baserCMS is a website development framework. Prior to version 4.8.0, there is a cross site	https://github.com/baserproject/basercms/commit/874c55433fead93e0be9df96fd28740f80	A-BAS-BASE-231123/109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request forgery vulnerability in the content preview feature of baserCMS. Version 4.8.0 contains a patch for this issue. **CVE ID : CVE-2023-43649**	47c8b6, https://basercms.net/security/JVN_99052047	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	30-Oct-2023	6.5	baserCMS is a website development framework. Prior to version 4.8.0, there is a Directory Traversal Vulnerability in the form submission data management feature of baserCMS. Version 4.8.0 contains a patch for this issue. **CVE ID : CVE-2023-43648**	https://basercms.net/security/JVN_81174674, https://github.com/baserproject/basercms/commit/7555a5cf0006755dc0223fffc2d882b50a97758b	A-BAS-BASE-231123/110
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	6.1	baserCMS is a website development framework with WebAPI that runs on PHP8 and CakePHP4. There is a XSS Vulnerability in Favorites Feature to baserCMS. This issue has been patched in version 4.8.0. **CVE ID : CVE-2023-29009**	https://basercms.net/security/JVN_45547161	A-BAS-BASE-231123/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Oct-2023	5.4	baserCMS is a website development framework. Prior to version 4.8.0, there is a cross-site scripting vulnerability in the file upload feature of baserCMS. Version 4.8.0 contains a patch for this issue. **CVE ID : CVE-2023-43647**	https://basercms.net/security/JVN_24381990	A-BAS-BASE-231123/112
Affected Version(s): From (including) 4.6.0 Up to (including) 4.7.6					
Improper Control of Generation of Code ('Code Injection')	30-Oct-2023	9.8	baserCMS is a website development framework. In versions 4.6.0 through 4.7.6, there is a Code Injection vulnerability in the mail form of baserCMS. As of time of publication, no known patched versions are available. **CVE ID : CVE-2023-43792**	https://basercms.net/security/JVN_45547161	A-BAS-BASE-231123/113
Vendor: bigbluebutton					
Product: bigbluebutton					
Affected Version(s): * Up to (excluding) 2.6.11					
Improper Neutralization of Input During	30-Oct-2023	5.4	BigBlueButton is an open-source virtual classroom. Prior to versions 2.6.11 and 2.7.0-	https://github.com/bigbluebutton/bigbluebutton/commit/304bc851a00558f9	A-BIG-BIGB-231123/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			beta.3, Guest Lobby was vulnerable to cross-site scripting when users wait to enter the meeting due to inserting unsanitized messages to the element using unsafe innerHTML. Text sanitizing was added for lobby messages starting in versions 2.6.11 and 2.7.0-beta.3. There are no known workarounds. **CVE ID : CVE-2023-43797**	9a908880f4ac44234a074c9d	
Affected Version(s): * Up to (including) 2.5.18					
Unrestricted Upload of File with Dangerous Type	30-Oct-2023	8.8	BigBlueButton is an open-source virtual classroom. BigBlueButton prior to version 2.6.0-beta.2 is vulnerable to unrestricted file upload, where the insertDocument API call does not validate the given file extension before saving the file, and does not remove it in case of validation failures. BigBlueButton 2.6.0-beta.2 contains a patch. There are no	N/A	A-BIG-BIGB-231123/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known workarounds. **CVE ID : CVE-2023-42803**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	30-Oct-2023	5.3	BigBlueButton is an open-source virtual classroom. BigBlueButton prior to version 2.6.0-beta.1 has a path traversal vulnerability that allows an attacker with a valid starting folder path, to traverse and read other files without authentication, assuming the files have certain extensions (txt, swf, svg, png). In version 2.6.0-beta.1, input validation was added on the parameters being passed and dangerous characters are stripped. There are no known workarounds. **CVE ID : CVE-2023-42804**	N/A	A-BIG-BIGB-231123/116
Affected Version(s): 2.6.0					
Unrestricted Upload of File with Dangerous Type	30-Oct-2023	8.8	BigBlueButton is an open-source virtual classroom. BigBlueButton prior to version	N/A	A-BIG-BIGB-231123/117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.6.0-beta.2 is vulnerable to unrestricted file upload, where the insertDocument API call does not validate the given file extension before saving the file, and does not remove it in case of validation failures. BigBlueButton 2.6.0-beta.2 contains a patch. There are no known workarounds. **CVE ID : CVE-2023-42803**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	30-Oct-2023	5.3	BigBlueButton is an open-source virtual classroom. BigBlueButton prior to version 2.6.0-beta.1 has a path traversal vulnerability that allows an attacker with a valid starting folder path, to traverse and read other files without authentication, assuming the files have certain extensions (txt, swf, svg, png). In version 2.6.0-beta.1, input validation was added on the	N/A	A-BIG-BIGB-231123/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameters being passed and dangerous characters are stripped. There are no known workarounds. **CVE ID : CVE-2023-42804**		
Affected Version(s): 2.7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Oct-2023	5.4	BigBlueButton is an open-source virtual classroom. Prior to versions 2.6.11 and 2.7.0-beta.3, Guest Lobby was vulnerable to cross-site scripting when users wait to enter the meeting due to inserting unsanitized messages to the element using unsafe innerHTML. Text sanitizing was added for lobby messages starting in versions 2.6.11 and 2.7.0-beta.3. There are no known workarounds. **CVE ID : CVE-2023-43797**	https://github.com/bigbluebutton/bigbluebutton/commit/304bc851a00558f99a908880f4ac44234a074c9d	A-BIG-BIGB-231123/119
Vendor: blmodules					
Product: csv_feeds_pro					
Affected Version(s): * Up to (excluding) 2.6.1					
Improper Neutralization of	31-Oct-2023	9.8	In the module "CSV Feeds PRO" (csvfeeds) before	https://security.friendsofpresta.org/modules/2	A-BLM-CSV_-231123/120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			2.6.1 from Bl Modules for PrestaShop, a guest can perform SQL injection. The method `SearchApiCsv::getProducts()` has sensitive SQL call that can be executed with a trivial http call and exploited to forge a SQL injection. **CVE ID : CVE-2023-46356**	023/10/26/csvfeeds-89.html	
Vendor: Blubrry					
Product: powerpress					
Affected Version(s): * Up to (excluding) 11.0.12					
N/A	16-Oct-2023	5.4	The PowerPress Podcasting plugin by Blubrry WordPress plugin before 11.0.12 does not sanitize and escape the media url field in posts, which could allow users with privileges as low as contributor to inject arbitrary web scripts that could target a site admin or superadmin. **CVE ID : CVE-2023-4820**	N/A	A-BLU-POWE-231123/121
Vendor: booking-wp-plugin					
Product: bookly					
Affected Version(s): * Up to (excluding) 22.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Oct-2023	7.2	The WordPress Online Booking and Scheduling Plugin WordPress plugin before 22.4 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin **CVE ID : CVE-2023-4691**	N/A	A-BOO-BOOK-231123/122
Vendor: booster					
Product: booster_for_woocommerce					
Affected Version(s): * Up to (excluding) 7.1.1					
Exposure of Sensitive Information to an Unauthorized Actor	20-Oct-2023	4.3	The Booster for WooCommerce for WordPress is vulnerable to Information Disclosure via the 'wcj_wp_option' shortcode in versions up to, and including, 7.1.0 due to insufficient controls on the information retrievable via the shortcode. This makes it possible for authenticated attackers, with subscriber-level capabilities or above, to retrieve arbitrary sensitive site options.	https://plugins.trac.wordpress.org/changeset/2966325/woocommerce-jetpack#file1, https://www.wordfence.com/threat-intel/vulnerabilities/id/a4cd49b2-ff93-4582-906b-b690d8472c38?source=cve	A-BOO-BOOS-231123/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4796		
Affected Version(s): * Up to (including) 7.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2023	5.4	The Booster for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'wcj_image' shortcode in versions up to, and including, 7.1.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5638**	https://plugins.trac.wordpress.org/browser/woocommerce-jetpack/tags/7.1.3/includes/shortcodes/class-wcj-general-shortcodes.php#L1122	A-BOO-BOOS-231123/124
Vendor: borbis					
Product: freshmail_for_wordpress					
Affected Version(s): * Up to (including) 2.3.2					
Improper Neutralization of Input During	26-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Borbis Media FreshMail For	N/A	A-BOR-FRES-231123/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			WordPress plugin <= 2.3.2 versions. **CVE ID : CVE-2023-46074**		
Vendor: bozdoz					
Product: leaflet_map					
Affected Version(s): * Up to (including) 3.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	The Leaflet Map plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 3.3.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5050**	https://plugins.trac.wordpress.org/changeset/2968965/leaflet-map#file12	A-BOZ-LEAF-231123/126
Vendor: brainstormforce					
Product: ultimate_addons_for_wpbakery_page_builder					
Affected Version(s): * Up to (excluding) 3.19.15					
Improper Neutralization of Input	27-Oct-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS)	N/A	A-BRA-ULTI-231123/127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			vulnerability in Brainstorm Force Ultimate Addons for WPBakery Page Builder plugin <= 3.19.14 versions. **CVE ID : CVE-2023-46211**		
Vendor: browserify					
Product: browserify-sign					
Affected Version(s): * Up to (excluding) 4.2.2					
Improper Verification of Cryptographic Signature	26-Oct-2023	7.5	browserify-sign is a package to duplicate the functionality of node's crypto public key functions, much of this is based on Fedor Indutny's work on indutny/tls.js. An upper bound check issue in `dsaVerify` function allows an attacker to construct signatures that can be successfully verified by any public key, thus leading to a signature forgery attack. All places in this project that involve DSA verification of user-input signatures will be affected by this vulnerability. This issue has been	N/A	A-BRO-BROW-231123/128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patched in version 4.2.2. **CVE ID : CVE-2023-46234**		
Vendor: buc					
Product: traceroute					
Affected Version(s): From (including) 2.0.12 Up to (excluding) 2.1.3					
N/A	25-Oct-2023	9.8	In buc Traceroute 2.0.12 through 2.1.2 before 2.1.3, the wrapper scripts do not properly parse command lines. **CVE ID : CVE-2023-46316**	N/A	A-BUC-TRAC-231123/129
Vendor: buddyboss					
Product: buddypress_global_search					
Affected Version(s): * Up to (including) 1.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in BuddyBoss BuddyPress Global Search plugin <= 1.2.1 versions. **CVE ID : CVE-2023-45755**	N/A	A-BUD-BUDD-231123/130
Vendor: busbaer					
Product: eisbaer_scada					
Affected Version(s): * Up to (including) 3.0.6433.1964					
Incorrect Permission Assignment for	25-Oct-2023	9.8	EisBaer Scada - CWE-732: Incorrect Permission	N/A	A-BUS-EISB-231123/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			Assignment for Critical Resource **CVE ID : CVE-2023-42489**		
Improper Authorization	25-Oct-2023	9.8	EisBaer Scada - CWE-285: Improper Authorization **CVE ID : CVE-2023-42491**	N/A	A-BUS-EISB-231123/132
Use of Hard-coded Credentials	25-Oct-2023	9.8	EisBaer Scada - CWE-321: Use of Hard-coded Cryptographic Key **CVE ID : CVE-2023-42492**	N/A	A-BUS-EISB-231123/133
Unprotected Storage of Credentials	25-Oct-2023	9.8	EisBaer Scada - CWE-256: Plaintext Storage of a Password **CVE ID : CVE-2023-42493**	N/A	A-BUS-EISB-231123/134
Exposed Dangerous Method or Function	25-Oct-2023	9.8	EisBaer Scada - CWE-749: Exposed Dangerous Method or Function **CVE ID : CVE-2023-42494**	N/A	A-BUS-EISB-231123/135
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Oct-2023	7.5	EisBaer Scada - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') **CVE ID : CVE-2023-42488**	N/A	A-BUS-EISB-231123/136
N/A	25-Oct-2023	7.5	EisBaer Scada - CWE-200:	N/A	A-BUS-EISB-231123/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exposure of Sensitive Information to an Unauthorized Actor **CVE ID : CVE-2023-42490**		
Vendor: buzzsprout					
Product: buzzsprout					
Affected Version(s): * Up to (excluding) 1.8.4					
N/A	30-Oct-2023	5.4	The Buzzsprout Podcasting plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'buzzsprout' shortcode in versions up to, and including, 1.8.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5335**	N/A	A-BUZ-BUZZ-231123/138
Vendor: byconsole					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wooodt_lite					
Affected Version(s): * Up to (including) 2.4.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ByConsole WooODT Lite – WooCommerce Order Delivery or Pickup with Date Time Location plugin <= 2.4.6 versions. **CVE ID : CVE-2023-45006**	N/A	A-BYC-WOOO-231123/139
Vendor: ca-ret					
Product: country_access_limit					
Affected Version(s): * Up to (including) 1.0.2					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Caret Inc. Caret Country Access Limit plugin <= 1.0.2 versions. **CVE ID : CVE-2023-45641**	N/A	A-CA--COUN-231123/140
Vendor: Calibre-ebook					
Product: calibre					
Affected Version(s): * Up to (excluding) 6.19.0					
Server-Side Request Forgery (SSRF)	22-Oct-2023	7.5	link_to_local_path in ebooks/conversion/plugins/html_input.py in calibre before 6.19.0 can, by default, add resources outside	N/A	A-CAL-CALI-231123/141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the document root. **CVE ID : CVE-2023-46303**		
Vendor: callrail					
Product: callrail_phone_call_tracking					
Affected Version(s): * Up to (including) 0.5.2					
N/A	27-Oct-2023	5.4	The CallRail Phone Call Tracking plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'callrail_form' shortcode in versions up to, and including, 0.5.2 due to insufficient input sanitization and output escaping on the 'form_id' user supplied attribute. This makes it possible for authenticated attackers with contributor level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5051**	https://plugins.trac.wordpress.org/changeset/2982876/callrail-phone-call-tracking#file0, https://www.wordfence.com/threat-intel/vulnerabilities/id/35def866-7460-4cad-8d86-7b9e4905cbe4?source=cve	A-CAL-CALL-231123/142
Vendor: carrcommunications					
Product: rsvpmaker					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 9.9.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	31-Oct-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in David F. Carr RSVPMaker allows SQL Injection.This issue affects RSVPMaker: from n/a through 9.9.3. **CVE ID : CVE-2023-25045**	N/A	A-CAR-RSVP-231123/143
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	31-Oct-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in David F. Carr RSVPMaker rsvpmaker allows SQL Injection.This issue affects RSVPMaker: from n/a through 9.9.3. **CVE ID : CVE-2023-25047**	N/A	A-CAR-RSVP-231123/144
Vendor: carrental_project					
Product: carrental					
Affected Version(s): 1.0					
Files or Directories Accessible to External Parties	23-Oct-2023	7.5	carRental 1.0 is vulnerable to Incorrect Access Control (Arbitrary File Read on the Back-end System).	N/A	A-CAR-CARR-231123/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33517		
Vendor: cassianetworks					
Product: access_controller					
Affected Version(s): 2.1.1.2303271039					
Improper Authentication	27-Oct-2023	8.8	An issue was discovered in Cassia Access Controller 2.1.1.2303271039. The Web SSH terminal endpoint (spawned console) can be accessed without authentication. Specifically, there is no session cookie validation on the Access Controller; instead, there is only Basic Authentication to the SSH console. **CVE ID : CVE-2023-35794**	N/A	A-CAS-ACCE-231123/146
Vendor: castos					
Product: seriously_simple_stats					
Affected Version(s): * Up to (including) 1.5.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Castos Seriously Simple Stats plugin <= 1.5.1 versions. **CVE ID : CVE-2023-45005**	N/A	A-CAS-SERI-231123/147
Vendor: chetangole					
Product: smooth_scroll_links					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.1.0					
Cross-Site Request Forgery (CSRF)	22-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Chetan Gole Smooth Scroll Links [SSL] plugin <= 1.1.0 versions. **CVE ID : CVE-2023-46095**	N/A	A-CHE-SMOO-231123/148
Vendor: Cisco					
Product: catalyst_sd-wan_manager					
Affected Version(s): 17.2.10					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 17.2.4					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 17.2.5					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 17.2.6					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20261		
Affected Version(s): 17.2.7					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 17.2.8					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/154
Affected Version(s): 17.2.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/155
Affected Version(s): 18.2.0					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco	https://sec.cloudapps.cisco.com	A-CIS-CATA-231123/156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	
Affected Version(s): 18.3.0					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could	https://sec.cloudapps.cisco.com/security/center/content/Cisco	A-CIS-CATA-231123/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	SecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	
Affected Version(s): 18.3.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-CATA-231123/158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	sdwan-lfi-OWLbKUGe	
Affected Version(s): 18.3.1.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 18.3.3					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 18.3.3.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 18.3.4					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 18.3.5					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 18.3.6.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 18.3.7					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 18.3.8					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 18.4.0					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 18.4.0.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 18.4.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 18.4.3					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 18.4.302					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 18.4.303					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 18.4.4					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 18.4.5					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20261		
Affected Version(s): 18.4.6					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 19.1.0					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/176
Affected Version(s): 19.2.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/177
Affected Version(s): 19.2.097					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco	https://sec.cloudapps.cisco.com	A-CIS-CATA-231123/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	
Affected Version(s): 19.2.099					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could	https://sec.cloudapps.cisco.com/security/center/content/Cisco	A-CIS-CATA-231123/179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	SecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	
Affected Version(s): 19.2.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-CATA-231123/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	sdwan-lfi-OWLbKUGe	
Affected Version(s): 19.2.2					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 19.2.3					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 19.2.31					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 19.2.4					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 19.2.929					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 19.3.0					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.1.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.1.1.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.1.12					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.1.2					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.1.3					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.3.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.3.2					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.3.2.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.3.3					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.3.3.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20261		
Affected Version(s): 20.3.4					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 20.3.4.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/198
Affected Version(s): 20.3.4.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/199
Affected Version(s): 20.3.4.3					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco	https://sec.cloudapps.cisco.com	A-CIS-CATA-231123/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	
Affected Version(s): 20.3.5					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could	https://sec.cloudapps.cisco.com/security/center/content/Cisco	A-CIS-CATA-231123/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	SecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	
Affected Version(s): 20.3.5.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-CATA-231123/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	sdwan-lfi-OWLbKUGe	
Affected Version(s): 20.3.6					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.3.7					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.3.7.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.3.7.2					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.3.8					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.4.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.4.1.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.4.1.2					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.4.2					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.4.2.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.4.2.2					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.4.2.3					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.5.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.5.1.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.5.1.2					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.6.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20261		
Affected Version(s): 20.6.1.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 20.6.1.2					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/220
Affected Version(s): 20.6.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/221
Affected Version(s): 20.6.2.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco	https://sec.cloudapps.cisco.com	A-CIS-CATA-231123/222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	
Affected Version(s): 20.6.2.2					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could	https://sec.cloudapps.cisco.com/security/center/content/Cisco	A-CIS-CATA-231123/223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	SecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	
Affected Version(s): 20.6.3					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-CATA-231123/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	sdwan-lfi-OWLbKUGe	
Affected Version(s): 20.6.3.0.45					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.6.3.0.46					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.6.3.0.47					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.6.3.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.6.3.2					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.6.3.3					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.6.3.4					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.6.4					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.6.4.0.21					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.6.4.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.6.4.2					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.6.5					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.6.5.1					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.6.5.1.10					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.6.5.1.11					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an authenticated user. **CVE ID : CVE-2023-20261**		
Affected Version(s): 20.6.5.1.13					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20261		
Affected Version(s): 20.6.5.1.7					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 20.6.5.1.9					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/242
Affected Version(s): 20.6.5.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/243
Affected Version(s): 20.6.5.2.4					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco	https://sec.cloudapps.cisco.com	A-CIS-CATA-231123/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	
Affected Version(s): 20.6.5.2.8					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could	https://sec.cloudapps.cisco.com/security/center/content/Cisco	A-CIS-CATA-231123/245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an authenticated, remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	SecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	
Affected Version(s): 20.6.5.4					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-CATA-231123/246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to retrieve arbitrary files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**	sdwan-lfi-OWLbKUGe	
Affected Version(s): 20.6.5.5					
N/A	18-Oct-2023	6.5	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to retrieve arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-lfi-OWLbKUGe	A-CIS-CATA-231123/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files from an affected system. This vulnerability is due to improper validation of parameters that are sent to the web UI. An attacker could exploit this vulnerability by logging in to Cisco Catalyst SD-WAN Manager and issuing crafted requests using the web UI. A successful exploit could allow the attacker to obtain arbitrary files from the underlying Linux file system of an affected system. To exploit this vulnerability, the attacker must be an authenticated user. **CVE ID : CVE-2023-20261**		
Vendor: Citrix					
Product: netscaler_application_delivery_controller					
Affected Version(s): From (including) 12.1 Up to (including) 12.1-55.300					
Improper Restriction of Operations within the Bounds of	27-Oct-2023	7.5	Denial of Service in NetScaler ADC and NetScaler Gateway when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP	https://support.citrix.com/article/CTX579459/	A-CIT-NETS-231123/248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Proxy) or AAA Virtual Server **CVE ID : CVE-2023-4967**		
Affected Version(s): From (including) 13.0 Up to (excluding) 13.0-92.19					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Oct-2023	7.5	Denial of Service in NetScaler ADC and NetScaler Gateway when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA Virtual Server **CVE ID : CVE-2023-4967**	https://support.citrix.com/article/CTX579459/	A-CIT-NETS-231123/249
Affected Version(s): From (including) 13.1 Up to (excluding) 13.1-49.15					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Oct-2023	7.5	Denial of Service in NetScaler ADC and NetScaler Gateway when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA Virtual Server **CVE ID : CVE-2023-4967**	https://support.citrix.com/article/CTX579459/	A-CIT-NETS-231123/250
Affected Version(s): From (including) 13.1 Up to (including) 13.1-37.164					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Oct-2023	7.5	Denial of Service in NetScaler ADC and NetScaler Gateway when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA Virtual Server **CVE ID : CVE-2023-4967**	https://support.citrix.com/article/CTX579459/	A-CIT-NETS-231123/251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 14.1 Up to (excluding) 14.1-8.50					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Oct-2023	7.5	Denial of Service in NetScaler ADC and NetScaler Gateway when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA Virtual Server **CVE ID : CVE-2023-4967**	https://support.citrix.com/article/CTX579459/	A-CIT-NETS-231123/252
Product: netscaler_gateway					
Affected Version(s): From (including) 13.0 Up to (excluding) 13.0-92.19					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Oct-2023	7.5	Denial of Service in NetScaler ADC and NetScaler Gateway when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA Virtual Server **CVE ID : CVE-2023-4967**	https://support.citrix.com/article/CTX579459/	A-CIT-NETS-231123/253
Affected Version(s): From (including) 13.1 Up to (excluding) 13.1-49.15					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Oct-2023	7.5	Denial of Service in NetScaler ADC and NetScaler Gateway when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA Virtual Server **CVE ID : CVE-2023-4967**	https://support.citrix.com/article/CTX579459/	A-CIT-NETS-231123/254
Affected Version(s): From (including) 14.1 Up to (excluding) 14.1-8.50					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Oct-2023	7.5	Denial of Service in NetScaler ADC and NetScaler Gateway when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA Virtual Server **CVE ID : CVE-2023-4967**	https://support.citrix.com/article/CTX579459/	A-CIT-NETS-231123/255
Vendor: clickdatos					
Product: proteccion_de_datos_rgpd					
Affected Version(s): * Up to (including) 3.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ClickDatos Protección de Datos RGPD plugin <= 3.1.0 versions. **CVE ID : CVE-2023-46071**	N/A	A-CLI-PROT-231123/256
Vendor: cmc3215					
Product: delete_me					
Affected Version(s): * Up to (including) 3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	The Delete Me plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'plugin_delete_me' shortcode in versions up to, and including, 3.0 due to insufficient input sanitization and output escaping on user supplied attributes.	https://plugins.trac.wordpress.org/browser/delete-me/tags/3.0/inc/shortcode.php#L83	A-CMC-DELE-231123/257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The shortcode is not displayed to administrators, so it cannot be used against administrator users. **CVE ID : CVE-2023-5126**		
Vendor: Cmsmadesimple					
Product: cms_made_simple					
Affected Version(s): 2.2.18					
N/A	26-Oct-2023	7.8	An issue in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted payload to the Content Manager Menu component. **CVE ID : CVE-2023-43352**	N/A	A-CMS-CMS_-231123/258
Improper Neutralization of Input During Web Page	20-Oct-2023	5.4	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary	N/A	A-CMS-CMS_-231123/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			code via a crafted script to the extra parameter in the news menu component. **CVE ID : CVE-2023-43353**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the Profiles parameter in the Extensions - MicroTiny WYSIWYG editor component. **CVE ID : CVE-2023-43354**	N/A	A-CMS-CMS_-231123/260
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the password and password again parameters in the My Preferences - Add user component. **CVE ID : CVE-2023-43355**	N/A	A-CMS-CMS_-231123/261
Improper Neutralization of Input	20-Oct-2023	5.4	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a	N/A	A-CMS-CMS_-231123/262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			local attacker to execute arbitrary code via a crafted script to the Global Meatadata parameter in the Global Settings Menu component. **CVE ID : CVE-2023-43356**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the Title parameter in the Manage Shortcuts component. **CVE ID : CVE-2023-43357**	N/A	A-CMS-CMS_-231123/263
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	5.4	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the Title parameter in the News Menu component. **CVE ID : CVE-2023-43358**	N/A	A-CMS-CMS_-231123/264
Improper Neutralization of Input During Web Page	19-Oct-2023	5.4	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary	N/A	A-CMS-CMS_-231123/265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			code via a crafted script to the Page Specific Metadata and Smarty data parameters in the Content Manager Menu component. **CVE ID : CVE-2023-43359**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	Cross Site Scripting vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted script to the Top Directory parameter in the File Picker Menu component. **CVE ID : CVE-2023-43360**	N/A	A-CMS-CMS_-231123/266
Vendor: codeastro					
Product: internet_banking_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Oct-2023	9.8	A vulnerability was found in CodeAstro Internet Banking System 1.0 and classified as critical. This issue affects some unknown processing of the file pages_reset_pwd.php. The manipulation of the argument email leads to sql injection. The	N/A	A-COD-INTE-231123/267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-243131. **CVE ID : CVE-2023-5693**		
Vendor: codedraft					
Product: mediabay_-_wordpress_media_library_folders					
Affected Version(s): * Up to (including) 1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-2023	5.4	Auth. (editor+) Stored Cross-Site Scripting (XSS) vulnerability in Codedrafty Mediabay – Media Library Folders plugin <= 1.6 versions. **CVE ID : CVE-2023-46066**	N/A	A-COD-MEDI-231123/268
Vendor: codedropz					
Product: drag_and_drop_multiple_file_uploader					
Affected Version(s): * Up to (excluding) 1.1.1					
N/A	16-Oct-2023	5.4	The Drag and Drop Multiple File Upload for WooCommerce WordPress plugin before 1.1.1 does not filter all potentially dangerous file extensions. Therefore, an attacker can	N/A	A-COD-DRAG-231123/269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upload unsafe .shtml or .svg files containing malicious scripts. **CVE ID : CVE-2023-4821**		
Vendor: Color					
Product: demoiccmax					
Affected Version(s): 2022-06-21					
Out-of-bounds Write	23-Oct-2023	8.8	In International Color Consortium DemoIccMAX 79ecb74, there is a stack-based buffer overflow in the icFixXml function in IccXML/IccLibXML/IccUtilXml.cpp in libIccXML.a. **CVE ID : CVE-2023-46602**	N/A	A-COL-DEMO-231123/270
Out-of-bounds Read	23-Oct-2023	7.8	In International Color Consortium DemoIccMAX 79ecb74, there is an out-of-bounds read in the CIccPRMG::GetChroma function in IccProfLib/IccPrmg.cpp in libSampleICC.a. **CVE ID : CVE-2023-46603**	N/A	A-COL-DEMO-231123/271
Out-of-bounds Write	30-Oct-2023	6.5	In International Color Consortium DemoIccMAX 79ecb74, CIccCLUT::Interp3d in	N/A	A-COL-DEMO-231123/272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IccProfLib/IccTagLut.cpp in libSampleICC.a attempts to access array elements at out-of-bounds indexes. **CVE ID : CVE-2023-46866**		
NULL Pointer Dereference	30-Oct-2023	6.5	In International Color Consortium DemoIccMAX 79ecb74, CIccXformMatrixTRC::GetCurve in IccCmm.cpp in libSampleICC.a has a NULL pointer dereference. **CVE ID : CVE-2023-46867**	N/A	A-COL-DEMO-231123/273
Vendor: Combodo					
Product: itop					
Affected Version(s): * Up to (excluding) 3.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	6.1	iTop is an open source, web-based IT service management platform. Prior to versions 3.0.4 and 3.1.0, on `pages/UI.php`, cross site scripting is possible. This issue is fixed in versions 3.0.4 and 3.1.0. **CVE ID : CVE-2023-34447**	https://github.com/Combodo/iTop/commit/519751faa10b2fc5b75ea4516a1b8ef13ca35b33, https://github.com/Combodo/iTop/commit/b8f61362f570e1ef8127175331012b7fc8aba802, https://github.com/Combodo/iTop/security/advisories/GHSA	A-COM-ITOP-231123/274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-6rfm-2rwg-mj7p	
Affected Version(s): 3.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	6.1	iTop is an open source, web-based IT service management platform. Prior to versions 3.0.4 and 3.1.0, when displaying `pages/preferences.php`, cross site scripting is possible. This issue is fixed in versions 3.0.4 and 3.1.0. **CVE ID : CVE-2023-34446**	https://github.com/Combodo/iTop/security/advisories/GHSA-q4pp-j46r-gm68, https://github.com/Combodo/iTop/commit/e3ba826e5dfd3b724f1ee97bebfd20ded3c70b10	A-COM-ITOP-231123/275
Vendor: common-services					
Product: sonice_etiquetage					
Affected Version(s): * Up to (including) 2.5.9					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-2023	7.5	In the module "SoNice etiquetage" (sonice_etiquetage) up to version 2.5.9 from Common-Services for PrestaShop, a guest can download personal information without restriction by performing a path traversal attack. Due to a lack of permissions control and a lack of control in the	https://security.friendsofpresta.org/modules/2023/10/17/sonice_etiquetage.html	A-COM-SONI-231123/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			path name construction, a guest can perform a path traversal to view all files on the information system. **CVE ID : CVE-2023-45383**		
Vendor: commscope					
Product: ruckus_cloudpath					
Affected Version(s): 5.12.54414					
Cross-Site Request Forgery (CSRF)	19-Oct-2023	9.6	A vulnerability in the web-based interface of the RUCKUS Cloudpath product on version 5.12 build 5538 or before to could allow a remote, unauthenticated attacker to execute persistent XSS and CSRF attacks against a user of the admin management interface. A successful attack, combined with a certain admin activity, could allow the attacker to gain full admin privileges on the exploited system. **CVE ID : CVE-2023-45992**	https://support.ruckuswireless.com/security_bulletins/322	A-COM-RUCK-231123/277
Vendor: concretecms					
Product: concrete_cms					
Affected Version(s): 9.2.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	5.4	Multiple Cross Site Scripting (XSS) vulnerabilities in Concrete CMS v.9.2.1 allow an attacker to execute arbitrary code via a crafted script to the Header and Footer Tracking Codes of the SEO & Statistics. **CVE ID : CVE-2023-44760**	N/A	A-CON-CONC-231123/278
Vendor: conversios					
Product: google_analytics_integration_for_woocommerce					
Affected Version(s): * Up to (excluding) 6.5.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Conversios Track Google Analytics 4, Facebook Pixel & Conversions API via Google Tag Manager for WooCommerce plugin <= 6.5.3 versions. **CVE ID : CVE-2023-46094**	N/A	A-CON-GOOG-231123/279
Vendor: coresol					
Product: snap_pixel					
Affected Version(s): * Up to (including) 1.5.7					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Hassan Ali Snap	N/A	A-COR-SNAP-231123/280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Pixel plugin <= 1.5.7 versions. **CVE ID : CVE-2023-45642**		
Vendor: covesa					
Product: dlt-daemon					
Affected Version(s): * Up to (including) 2.18.8					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Oct-2023	7.5	Connected Vehicle Systems Alliance (COVESA) up to v2.18.8 was discovered to contain a buffer overflow via the component /shared/dlt_common.c. **CVE ID : CVE-2023-36321**	https://github.com/michael-methner/dlt-daemon/commit/8ac9a080bee25e67e49bd138d81c992ce7b6d899	A-COV-DLT--231123/281
Vendor: craterapp					
Product: crater					
Affected Version(s): * Up to (including) 6.0.6					
Improper Control of Generation of Code ('Code Injection')	30-Oct-2023	7.2	/api/v1/company/upload-logo in CompanyController.php in crater through 6.0.6 allows a superadmin to execute arbitrary PHP code by placing this code into an image/png IDAT chunk of a Company Logo image. **CVE ID : CVE-2023-46865**	https://github.com/crater-invoice/crater/pull/1271, https://github.com/crater-invoice/crater/issues/1267	A-CRA-CRAT-231123/282
Vendor: crypto-js_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: crypto-js					
Affected Version(s): * Up to (excluding) 4.2.0					
Use of a Broken or Risky Cryptographic Algorithm	25-Oct-2023	9.1	crypto-js is a JavaScript library of crypto standards. Prior to version 4.2.0, crypto-js PBKDF2 is 1,000 times weaker than originally specified in 1993, and at least 1,300,000 times weaker than current industry standard. This is because it both defaults to SHA1, a cryptographic hash algorithm considered insecure since at least 2005, and defaults to one single iteration, a 'strength' or 'difficulty' value specified at 1,000 when specified in 1993. PBKDF2 relies on iteration count as a countermeasure to preimage and collision attacks. If used to protect passwords, the impact is high. If used to generate signatures, the impact is high. Version 4.2.0 contains a patch	https://github.com/brix/crypto-js/security/advisories/GHSA-xwcq-pm8m-c4vf, https://github.com/brix/crypto-js/commit/421dd538b2d34e7c24a5b72cc64dc2b9167db40a	A-CRY-CRYP-231123/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for this issue. As a workaround, configure crypto-js to use SHA256 with at least 250,000 iterations. **CVE ID : CVE-2023-46233**		
Vendor: cti_monitoring_and_early_warning_system_project					
Product: cti_monitoring_and_early_warning_system					
Affected Version(s): 2.2					
N/A	27-Oct-2023	9.8	A vulnerability was found in Shanghai CTI Navigation CTI Monitoring and Early Warning System 2.2. It has been classified as critical. This affects an unknown part of the file /Web/SysManage/UserEdit.aspx. The manipulation of the argument ID leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-243717 was assigned to this vulnerability. **CVE ID : CVE-2023-5827**	N/A	A-CTI-CTI_-231123/284
Vendor: cytechmobile					
Product: buddymeet					
Affected Version(s): * Up to (excluding) 2.3.0					
Improper Neutralization of	16-Oct-2023	5.4	Auth. (contributo+) Stored Cross-Site Scripting (XSS)	N/A	A-CYT-BUDD-231123/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			vulnerability in Cytech BuddyMeet plugin <= 2.2.0 versions. **CVE ID : CVE-2023-44985**		
Vendor: davidlingren					
Product: media_library_assistant					
Affected Version(s): * Up to (excluding) 3.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	4.8	Auth. (author+) Stored Cross-Site Scripting (XSS) vulnerability in David Lingren Media Library Assistant plugin <= 3.11 versions. **CVE ID : CVE-2023-24385**	N/A	A-DAV-MEDI-231123/286
Vendor: dbcli					
Product: mycli					
Affected Version(s): 1.27.0					
Inadequate Encryption Strength	19-Oct-2023	7.5	Inadequate encryption strength in mycli 1.27.0 allows attackers to view sensitive information via /mycli/config.py **CVE ID : CVE-2023-44690**	N/A	A-DBC-MYCL-231123/287
Vendor: deanoakley					
Product: photospace_responsive_gallery					
Affected Version(s): * Up to (excluding) 2.2.0					
Improper Neutralization of Input	20-Oct-2023	4.8	The Photospace Responsive plugin for WordPress is vulnerable to	https://www.wordfence.com/threat-intel/vulnerabil	A-DEA-PHOT-231123/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Stored Cross-Site Scripting via the 'psres_button_size' parameter in versions up to, and including, 2.1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-4271**	ities/id/3bc98896-6ff9-40de-ace2-2ca331c2a44a?source=cve	
Vendor: Dell					
Product: unityvsa_operating_environment					
Affected Version(s): * Up to (excluding) 5.3.0.0.5.120					
Improper Neutralization of Special Elements used in an OS Command ('OS	23-Oct-2023	7.8	Dell Unity prior to 5.3 contains a Restricted Shell Bypass vulnerability. This could allow an authenticated, local attacker to exploit	https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-	A-DEL-UNIT-231123/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			this vulnerability by authenticating to the device CLI and issuing certain commands. **CVE ID : CVE-2023-43066**	update-for-multiple-vulnerabilities	
N/A	23-Oct-2023	7.5	Dell Unity 5.3 contain(s) an Arbitrary File Creation vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability by crafting arbitrary files through a request to the server. **CVE ID : CVE-2023-43074**	https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities	A-DEL-UNIT-231123/290
Improper Restriction of XML External Entity Reference	23-Oct-2023	6.5	Dell Unity prior to 5.3 contains an XML External Entity injection vulnerability. An XXE attack could potentially exploit this vulnerability disclosing local files in the file system.	https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities	A-DEL-UNIT-231123/291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43067		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	5.4	Dell Unity prior to 5.3 contains a Cross-site scripting vulnerability. A low-privileged authenticated attacker can exploit these issues to obtain escalated privileges. **CVE ID : CVE-2023-43065**	https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities	A-DEL-UNIT-231123/292
Product: unity_operating_environment					
Affected Version(s): * Up to (excluding) 5.3.0.0.5.120					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Oct-2023	7.8	Dell Unity prior to 5.3 contains a Restricted Shell Bypass vulnerability. This could allow an authenticated, local attacker to exploit this vulnerability by authenticating to the device CLI and issuing certain commands. **CVE ID : CVE-2023-43066**	https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities	A-DEL-UNIT-231123/293
N/A	23-Oct-2023	7.5		https://www.dell.com/support/kbdoc/en-	A-DEL-UNIT-231123/294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Dell Unity 5.3 contain(s) an Arbitrary File Creation vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability by crafting arbitrary files through a request to the server. **CVE ID : CVE-2023-43074**	us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities	
Improper Restriction of XML External Entity Reference	23-Oct-2023	6.5	Dell Unity prior to 5.3 contains an XML External Entity injection vulnerability. An XXE attack could potentially exploit this vulnerability disclosing local files in the file system. **CVE ID : CVE-2023-43067**	https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities	A-DEL-UNIT-231123/295
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	5.4	Dell Unity prior to 5.3 contains a Cross-site scripting vulnerability. A low-privileged authenticated attacker can exploit these issues to obtain escalated privileges.	https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities	A-DEL-UNIT-231123/296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43065		
Product: unity_xt_operating_environment					
Affected Version(s): * Up to (excluding) 5.3.0.0.5.120					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Oct-2023	7.8	Dell Unity prior to 5.3 contains a Restricted Shell Bypass vulnerability. This could allow an authenticated, local attacker to exploit this vulnerability by authenticating to the device CLI and issuing certain commands. **CVE ID : CVE-2023-43066**	https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities	A-DEL-UNIT-231123/297
N/A	23-Oct-2023	7.5	Dell Unity 5.3 contain(s) an Arbitrary File Creation vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability by crafting arbitrary files through a request to the server. **CVE ID : CVE-2023-43074**	https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities	A-DEL-UNIT-231123/298
Improper Restriction of XML External	23-Oct-2023	6.5	Dell Unity prior to 5.3 contains an XML External	https://www.dell.com/support/kbdoc/en-us/000213152/	A-DEL-UNIT-231123/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Entity Reference			Entity injection vulnerability. An XXE attack could potentially exploit this vulnerability disclosing local files in the file system. **CVE ID : CVE-2023-43067**	dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	5.4	Dell Unity prior to 5.3 contains a Cross-site scripting vulnerability. A low-privileged authenticated attacker can exploit these issues to obtain escalated privileges. **CVE ID : CVE-2023-43065**	https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities	A-DEL-UNIT-231123/300
Vendor: devolutions					
Product: devolutions_server					
Affected Version(s): * Up to (including) 2022.3.13.0					
N/A	16-Oct-2023	6.5	Improper access control in the permission inheritance in Devolutions Server 2022.3.13.0 and earlier allows an attacker that compromised a low privileged user to access entries via a	https://devolutions.net/security/advisories/DEVO-2023-0018	A-DEV-DEVO-231123/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific combination of permissions in the entry and in its parent. **CVE ID : CVE-2023-5575**		
Vendor: dexma					
Product: dexgate					
Affected Version(s): 20130114					
Improper Authentication	19-Oct-2023	8.8	The affected product is vulnerable to an improper authentication vulnerability, which may allow an attacker to impersonate a legitimate user as long as the device keeps the session active, since the attack takes advantage of the cookie header to generate "legitimate" requests. **CVE ID : CVE-2023-41089**	N/A	A-DEX-DEXG-231123/302
Cross-Site Request Forgery (CSRF)	19-Oct-2023	8.8	The affected product is vulnerable to a cross-site request forgery vulnerability, which may allow an attacker to perform actions with the	N/A	A-DEX-DEXG-231123/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permissions of a victim user. **CVE ID : CVE-2023-42435**		
Cleartext Transmission of Sensitive Information	19-Oct-2023	6.5	The affected product is vulnerable to a cleartext transmission of sensitive information vulnerability, which may allow an attacker with access to the network, where clients have access to the DexGate server, could capture traffic. The attacker can later us the information within it to access the application. **CVE ID : CVE-2023-41088**	N/A	A-DEX-DEXG-231123/304
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2023	6.1	The affected product is vulnerable to a cross-site scripting vulnerability, which could allow an attacker to access the web application to introduce arbitrary Java Script by injecting an XSS payload into the 'hostname'	N/A	A-DEX-DEXG-231123/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter of the vulnerable software. **CVE ID : CVE-2023-40153**		
N/A	19-Oct-2023	5.3	The affected product is vulnerable to an exposure of sensitive information to an unauthorized actor vulnerability, which may allow an attacker to create malicious requests for obtaining the information of the version about the web server used. **CVE ID : CVE-2023-42666**	N/A	A-DEX-DEXG-231123/306
Vendor: discourse					
Product: discourse					
Affected Version(s): * Up to (including) 3.1.1					
Uncontrolled Resource Consumption	16-Oct-2023	7.5	Discourse is an open source platform for community discussion. A malicious request can cause production log files to quickly fill up and thus result in the server running out of disk space. This problem has been patched in the	https://github.com/discourse/discourse/security/advisories/GHSA-89h3-g746-xmwq	A-DIS-DISC-231123/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1.1 stable and 3.2.0.beta2 versions of Discourse. It is possible to temporarily work around this problem by reducing the `client_max_body_size nginx directive`. `client_max_body_size` will limit the size of uploads that can be uploaded directly to the server. **CVE ID : CVE-2023-44388**		
N/A	16-Oct-2023	7.5	Discourse is an open source platform for community discussion. New chat messages can be read by making an unauthenticated POST request to MessageBus. This issue is patched in the 3.1.1 stable and 3.2.0.beta2 versions of Discourse. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45131**	https://github.com/discourse/discourse/security/advisories/GHSA-84gf-hhrc-9pw6	A-DIS-DISC-231123/308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-2023	5.4	Discourse is an open source platform for community discussion. Improper escaping of user input allowed for Cross-site Scripting attacks via the digest email preview UI. This issue only affects sites with CSP disabled. This issue has been patched in the 3.1.1 stable release as well as the 3.2.0.beta1 release. Users are advised to upgrade. Users unable to upgrade should ensure CSP is enabled on the forum. **CVE ID : CVE-2023-43659**	https://github.com/discourse/discourse/security/advisories/GHSA-g4qg-5q2h-m8ph	A-DIS-DISC-231123/309
N/A	16-Oct-2023	5.3	Discourse is an open source platform for community discussion. User summaries are accessible for anonymous users even when `hide_user_profiles_from_public` is enabled. This problem has been patched in the 3.1.1	https://github.com/discourse/discourse/security/advisories/GHSA-7px5-fqcf-7mfr	A-DIS-DISC-231123/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stable and 3.2.0.beta2 version of Discourse. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-44391**		
N/A	16-Oct-2023	3.7	Discourse is an open source platform for community discussion. Attackers with details specific to a poll in a topic can use the `/polls/grouped_poll_results` endpoint to view the content of options in the poll and the number of votes for groups of poll participants. This impacts private polls where the results were intended to only be viewable by authorized users. This issue is patched in the 3.1.1 stable and 3.2.0.beta2 versions of Discourse. There is no workaround for this issue apart from upgrading to the fixed version.	https://github.com/discourse/discourse/security/advisories/GHSA-3x57-846g-7qcw	A-DIS-DISC-231123/311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43814		
N/A	16-Oct-2023	3.1	Discourse is an open source community platform. In affected versions any user can create a topic and add arbitrary custom fields to a topic. The severity of this vulnerability depends on what plugins are installed and how the plugins uses topic custom fields. For a default Discourse installation with the default plugins, this vulnerability has no impact. The problem has been patched in the latest version of Discourse. Users are advised to update to version 3.1.1 if they are on the stable branch or 3.2.0.beta2 if they are on the beta branch. Users unable to upgrade should disable any plugins that access topic custom fields. **CVE ID : CVE-2023-45147**	https://github.com/discourse/discourse/security/advisories/GHSA-wm89-m359-f9qv	A-DIS-DISC-231123/312
Affected Version(s): 3.2.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	16-Oct-2023	7.5	Discourse is an open source platform for community discussion. A malicious request can cause production log files to quickly fill up and thus result in the server running out of disk space. This problem has been patched in the 3.1.1 stable and 3.2.0.beta2 versions of Discourse. It is possible to temporarily work around this problem by reducing the `client_max_body_size nginx directive`. `client_max_body_size` will limit the size of uploads that can be uploaded directly to the server. **CVE ID : CVE-2023-44388**	https://github.com/discourse/discourse/security/advisories/GHSA-89h3-g746-xmwq	A-DIS-DISC-231123/313
N/A	16-Oct-2023	7.5	Discourse is an open source platform for community discussion. New chat messages can be read by making an unauthenticated POST request to MessageBus. This	https://github.com/discourse/discourse/security/advisories/GHSA-84gf-hhrc-9pw6	A-DIS-DISC-231123/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is patched in the 3.1.1 stable and 3.2.0.beta2 versions of Discourse. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45131**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-2023	5.4	Discourse is an open source platform for community discussion. Improper escaping of user input allowed for Cross-site Scripting attacks via the digest email preview UI. This issue only affects sites with CSP disabled. This issue has been patched in the 3.1.1 stable release as well as the 3.2.0.beta1 release. Users are advised to upgrade. Users unable to upgrade should ensure CSP is enabled on the forum. **CVE ID : CVE-2023-43659**	https://github.com/discourse/discourse/security/advisories/GHSA-g4qg-5q2h-m8ph	A-DIS-DISC-231123/315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Oct-2023	5.3	Discourse is an open source platform for community discussion. User summaries are accessible for anonymous users even when `hide_user_profiles_from_public` is enabled. This problem has been patched in the 3.1.1 stable and 3.2.0.beta2 version of Discourse. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-44391**	https://github.com/discourse/discourse/security/advisories/GHSA-7px5-fqcf-7mfr	A-DIS-DISC-231123/316
N/A	16-Oct-2023	3.7	Discourse is an open source platform for community discussion. Attackers with details specific to a poll in a topic can use the `/polls/grouped_poll_results` endpoint to view the content of options in the poll and the number of votes for groups of poll participants. This impacts private polls where the	https://github.com/discourse/discourse/security/advisories/GHSA-3x57-846g-7qcw	A-DIS-DISC-231123/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			results were intended to only be viewable by authorized users. This issue is patched in the 3.1.1 stable and 3.2.0.beta2 versions of Discourse. There is no workaround for this issue apart from upgrading to the fixed version. **CVE ID : CVE-2023-43814**		
N/A	16-Oct-2023	3.1	Discourse is an open source community platform. In affected versions any user can create a topic and add arbitrary custom fields to a topic. The severity of this vulnerability depends on what plugins are installed and how the plugins uses topic custom fields. For a default Discourse installation with the default plugins, this vulnerability has no impact. The problem has been patched in the latest version of Discourse. Users	https://github.com/discourse/discourse/security/advisories/GHSA-wm89-m359-f9qv	A-DIS-DISC-231123/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are advised to update to version 3.1.1 if they are on the stable branch or 3.2.0.beta2 if they are on the beta branch. Users unable to upgrade should disable any plugins that access topic custom fields. **CVE ID : CVE-2023-45147**		
Product: discourse_calendar					
Affected Version(s): * Up to (including) 2023-10-16					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-2023	6.1	dicourse-calendar is a plugin for the Discourse messaging platform which adds the ability to create a dynamic calendar in the first post of a topic. Improper escaping of event titles could lead to Cross-site Scripting (XSS) within the 'email preview' UI when a site has CSP disabled. Having CSP disabled is a non-default configuration, so the vast majority of sites are unaffected. This problem is resolved in the latest version of the discourse-calendar plugin.	https://github.com/discourse/discourse-calendar/commit/9788310906febb36822d6823d14f1059c39644de, https://github.com/discourse/discourse-calendar/security/advisories/GHSA-3fwj-f6ww-7hr6	A-DIS-DISC-231123/319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Users are advised to upgrade. Users unable to upgrade should ensure CSP is enabled on the forum. **CVE ID : CVE-2023-43658**		
Vendor: dmconcept					
Product: configurator					
Affected Version(s): * Up to (excluding) 4.9.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Oct-2023	9.8	DM Concept configurator before v4.9.4 was discovered to contain a SQL injection vulnerability via the component ConfiguratorAttachment::getAttachmentByToken. **CVE ID : CVE-2023-43986**	N/A	A-DMC-CONF-231123/320
Vendor: documentlocator					
Product: document_locator					
Affected Version(s): * Up to (excluding) 7.2					
N/A	27-Oct-2023	9.8	A vulnerability classified as critical has been found in ColumbiaSoft Document Locator. This affects an unknown part of the file /api/authentication/login of the component WebTools. The manipulation of the argument Server	N/A	A-DOC-DOCU-231123/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to improper authentication. It is possible to initiate the attack remotely. Upgrading to version 7.2 SP4 and 2021.1 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-243729 was assigned to this vulnerability. **CVE ID : CVE-2023-5830**		
Affected Version(s): 21					
N/A	27-Oct-2023	9.8	A vulnerability classified as critical has been found in ColumbiaSoft Document Locator. This affects an unknown part of the file /api/authentication/login of the component WebTools. The manipulation of the argument Server leads to improper authentication. It is possible to initiate the attack remotely. Upgrading to version 7.2 SP4 and 2021.1 is able	N/A	A-DOC-DOCU-231123/322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to address this issue. It is recommended to upgrade the affected component. The identifier VDB-243729 was assigned to this vulnerability. **CVE ID : CVE-2023-5830**		
Affected Version(s): 7.2					
N/A	27-Oct-2023	9.8	A vulnerability classified as critical has been found in ColumbiaSoft Document Locator. This affects an unknown part of the file /api/authentication/login of the component WebTools. The manipulation of the argument Server leads to improper authentication. It is possible to initiate the attack remotely. Upgrading to version 7.2 SP4 and 2021.1 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-243729 was	N/A	A-DOC-DOCU-231123/323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. **CVE ID : CVE-2023-5830**		
Vendor: Dolibarr					
Product: dolibarr_erp\/crm					
Affected Version(s): * Up to (excluding) 16.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Oct-2023	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository dolibarr/dolibarr prior to 16.0.5. **CVE ID : CVE-2023-5842**	https://huntr.com/bounties/aed81114-5952-46f5-ae3a-e66518e98ba3, https://github.com/dolibarr/dolibarr/commit/f569048eb2bd823525bce4ef52316e7a83e3345c	A-DOL-DOLI-231123/324
Vendor: dom4j_project					
Product: dom4j					
Affected Version(s): * Up to (including) 2.1.4					
XML Injection (aka Blind XPath Injection)	25-Oct-2023	7.5	An issue in dom4j org.dom4j.io.SAXReader v.2.1.4 and before allows a remote attacker to obtain sensitive information via the setFeature function. NOTE: the vendor and original reporter indicate that this is not a vulnerability because setFeature only sets features, which "can be safe in one case and unsafe in another."	N/A	A-DOM-DOM4-231123/325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45960		
Vendor: Dotcms					
Product: dotcms					
Affected Version(s): 21.06					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	6.1	In dotCMS, versions mentioned, a flaw in the NormalizationFilter does not strip double slashes (//) from URLs, potentially enabling bypasses for XSS and access controls. An example affected URL is https://demo.dotcms.com//html/portlet/ext/files/edit_text_inc.jsp https://demo.dotcms.com//html/portlet/ext/files/edit_text_inc.jsp , which should return a 404 response but didn't. The oversight in the default invalid URL character list can be viewed at the provided GitHub link https://github.com/dotCMS/core/blob/master/dotCMS/src/main/java/com/dotcms/filters/	https://www.dotcms.com/security/SI-68	A-DOT-DOTC-231123/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NormalizationFilter.java#L37 . To mitigate, users can block URLs with double slashes at firewalls or utilize dotCMS config variables. Specifically, they can use the DOT_URI_NORMALIZATION_FORBIDDEN_STRINGS environmental variable to add // to the list of invalid strings. Additionally, the DOT_URI_NORMALIZATION_FORBIDDEN_REGEX variable offers more detailed control, for instance, to block //html.* URLs. Fix Version:23.06+, LTS 22.03.7+, LTS 23.01.4+ **CVE ID : CVE-2023-3042**		
Affected Version(s): 22.03					
Improper Neutralization of Input During Web Page Generation	17-Oct-2023	6.1	In dotCMS, versions mentioned, a flaw in the NormalizationFilter does not strip double slashes (//) from URLs,	https://www.dotcms.com/security/SI-68	A-DOT-DOTC-231123/327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			potentially enabling bypasses for XSS and access controls. An example affected URL is https://demo.dotcms.com//html/portlet/ext/files/edit_text_inc.jsp https://demo.dotcms.com//html/portlet/ext/files/edit_text_inc.jsp , which should return a 404 response but didn't. The oversight in the default invalid URL character list can be viewed at the provided GitHub link https://github.com/dotCMS/core/blob/master/dotCMS/src/main/java/com/dotcms/filters/NormalizationFilter.java#L37 . To mitigate, users can block URLs with double slashes at firewalls or utilize dotCMS config variables. Specifically, they can use the DOT_URI_NORMALIZATION_FORBIDDEN_STRINGS environmental variable to add //		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the list of invalid strings. Additionally, the DOT_URI_NORMALIZATION_FORBIDDEN_REGEX variable offers more detailed control, for instance, to block //html.* URLs. Fix Version:23.06+, LTS 22.03.7+, LTS 23.01.4+ **CVE ID : CVE-2023-3042**		
Affected Version(s): 23.01					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	6.1	In dotCMS, versions mentioned, a flaw in the NormalizationFilter does not strip double slashes (//) from URLs, potentially enabling bypasses for XSS and access controls. An example affected URL is https://demo.dotcms.com//html/portlet/ext/files/edit_text_inc.jsp https://demo.dotcms.com//html/portlet/ext/files/edit_text_inc.jsp , which should return a 404 response but didn't.	https://www.dotcms.com/security/SI-68	A-DOT-DOTC-231123/328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The oversight in the default invalid URL character list can be viewed at the provided GitHub link https://github.com/dotCMS/core/blob/master/dotCMS/src/main/java/com/dotcms/filters/NormalizationFilter.java#L37 . To mitigate, users can block URLs with double slashes at firewalls or utilize dotCMS config variables. Specifically, they can use the DOT_URI_NORMALIZATION_FORBIDDEN_STRINGS environmental variable to add // to the list of invalid strings. Additionally, the DOT_URI_NORMALIZATION_FORBIDDEN_REGEX variable offers more detailed control, for instance, to block //html.* URLs. Fix Version:23.06+, LTS 22.03.7+, LTS 23.01.4+ **CVE ID : CVE-2023-3042**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 5.3.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	6.1	In dotCMS, versions mentioned, a flaw in the NormalizationFilter does not strip double slashes (//) from URLs, potentially enabling bypasses for XSS and access controls. An example affected URL is https://demo.dotcms.com//html/portlet/ext/files/edit_text_inc.jsp https://demo.dotcms.com//html/portlet/ext/files/edit_text_inc.jsp , which should return a 404 response but didn't. The oversight in the default invalid URL character list can be viewed at the provided GitHub link https://github.com/dotCMS/core/blob/master/dotCMS/src/main/java/com/dotcms/filters/NormalizationFilter.java#L37 . To mitigate, users can block URLs with double slashes at firewalls	https://www.dotcms.com/security/SI-68	A-DOT-DOTC-231123/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or utilize dotCMS config variables. Specifically, they can use the DOT_URI_NORMALIZATION_FORBIDDEN_STRINGS environmental variable to add // to the list of invalid strings. Additionally, the DOT_URI_NORMALIZATION_FORBIDDEN_REGEX variable offers more detailed control, for instance, to block //html.* URLs. Fix Version:23.06+, LTS 22.03.7+, LTS 23.01.4+ **CVE ID : CVE-2023-3042**		
Vendor: dreamer_cms_project					
Product: dreamer_cms					
Affected Version(s): 4.1.3					
Cross-Site Request Forgery (CSRF)	17-Oct-2023	8.8	Dreamer CMS v4.1.3 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin\/category\/add. **CVE ID : CVE-2023-45901**	N/A	A-DRE-DREA-231123/330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	17-Oct-2023	8.8	Dreamer CMS v4.1.3 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/attachment/delete. **CVE ID : CVE-2023-45902**	N/A	A-DRE-DREA-231123/331
Cross-Site Request Forgery (CSRF)	17-Oct-2023	8.8	Dreamer CMS v4.1.3 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/label/delete. **CVE ID : CVE-2023-45903**	N/A	A-DRE-DREA-231123/332
Cross-Site Request Forgery (CSRF)	17-Oct-2023	8.8	Dreamer CMS v4.1.3 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /variable/update. **CVE ID : CVE-2023-45904**	N/A	A-DRE-DREA-231123/333
Cross-Site Request Forgery (CSRF)	17-Oct-2023	8.8	Dreamer CMS v4.1.3 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/variable/add.	N/A	A-DRE-DREA-231123/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45905		
Cross-Site Request Forgery (CSRF)	17-Oct-2023	8.8	Dreamer CMS v4.1.3 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/user/add. **CVE ID : CVE-2023-45906**	N/A	A-DRE-DREA-231123/335
Cross-Site Request Forgery (CSRF)	17-Oct-2023	8.8	Dreamer CMS v4.1.3 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/variable/delete. **CVE ID : CVE-2023-45907**	N/A	A-DRE-DREA-231123/336
Vendor: dreamsecurity					
Product: magicline_4.0					
Affected Version(s): From (including) 1.0.0.1 Up to (including) 1.0.0.26					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Oct-2023	9.8	A Buffer overflow vulnerability in DreamSecurity MagicLine4NX versions 1.0.0.1 to 1.0.0.26 allows an attacker to remotely execute code. **CVE ID : CVE-2023-45797**	N/A	A-DRE-MAGI-231123/337
Vendor: dromara					
Product: sa-token					
Affected Version(s): * Up to (excluding) 1.36.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	25-Oct-2023	8.8	An issue in Dromara SaToken version 1.3.50RC and before when using Spring dynamic controllers, a specially crafted request may cause an authentication bypass. **CVE ID : CVE-2023-43961**	N/A	A-DRO-SA-T-231123/338
Affected Version(s): * Up to (excluding) 1.37.0					
N/A	25-Oct-2023	9.8	An issue in Dromara SaToken version 1.36.0 and before allows a remote attacker to escalate privileges via a crafted payload to the URL. **CVE ID : CVE-2023-44794**	https://github.com/dromara/Sa-Token/issues/515	A-DRO-SA-T-231123/339
Product: sureness					
Affected Version(s): * Up to (excluding) 1.0.8					
Use of Hard-coded Credentials	25-Oct-2023	9.8	Dromara Sureness before v1.0.8 was discovered to use a hardcoded key. **CVE ID : CVE-2023-31581**	N/A	A-DRO-SURE-231123/340
Vendor: e-invoice_project					
Product: e-invoice					
Affected Version(s): * Up to (excluding) 2.1					
Improper Protection for Out of Bounds Signal	27-Oct-2023	7.5	Improper Protection for Outbound Error Messages and Alert Signals	N/A	A-E-I-E-IN-231123/341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Level Alerts			vulnerability in EDM Informatics E-invoice allows Account Footprinting.This issue affects E-invoice: before 2.1. **CVE ID : CVE-2023-5443**		
Vendor: easyuse					
Product: mailhunter_ultimate					
Affected Version(s): * Up to (including) 2023					
Unrestricted Upload of File with Dangerous Type	17-Oct-2023	8.8	Unrestricted upload of file with dangerous type vulnerability in create template function in EasyUse MailHunter Ultimate 2023 and earlier allows remote authenticated users to perform arbitrary system commands with 'NT Authority\SYSTEM' privilege via a crafted ZIP archive. **CVE ID : CVE-2023-34207**	N/A	A-EAS-MAIL-231123/342
Improper Neutralization of Special Elements used in an SQL Command	17-Oct-2023	8.8	SQL Injection in create customer group function in EasyUse MailHunter Ultimate 2023 and earlier allow remote authenticated	N/A	A-EAS-MAIL-231123/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			users to execute arbitrary SQL commands via the ctl00$ContentPlaceHolder1$txtCustSQL parameter. **CVE ID : CVE-2023-34210**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Oct-2023	6.5	Path Traversal in create template function in EasyUse MailHunter Ultimate 2023 and earlier allow remote authenticated users to extract files into arbitrary directories via a crafted ZIP archive. **CVE ID : CVE-2023-34208**	N/A	A-EAS-MAIL-231123/344
N/A	17-Oct-2023	4.3	Exposure of Sensitive System Information to an Unauthorized Control Sphere in create template function in EasyUse MailHunter Ultimate 2023 and earlier allow remote authenticated users to obtain the absolute path via unencrypted VIEWSTATE parameter.	N/A	A-EAS-MAIL-231123/345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34209		
Vendor: Eaton					
Product: easysoft					
Affected Version(s): * Up to (excluding) 8.01					
Insufficiently Protected Credentials	17-Oct-2023	6.5	Eaton easySoft software is used to program easy controllers and displays for configuring, programming and defining parameters for all the intelligent relays. This software has a password protection functionality to secure the project file from unauthorized access. This password was being stored insecurely and could be retrieved by skilled adversaries. **CVE ID : CVE-2023-43777**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1011.pdf	A-EAT-EASY-231123/346
Vendor: Eclipse					
Product: mosquitto					
Affected Version(s): * Up to (excluding) 2.0.6					
Excessive Iteration	18-Oct-2023	7.5	In Eclipse Mosquitto before and including 2.0.5, establishing a connection to the mosquitto server	https://github.com/eclipse/mosquitto/commit/18bad1ff32435e523d7507e9	A-ECL-MOSQ-231123/347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without sending data causes the EPOLLOUT event to be added, which results excessive CPU consumption. This could be used by a malicious actor to perform denial of service type attack. This issue is fixed in 2.0.6 **CVE ID : CVE-2023-5632**	b2ce0010124a8f2d	
Vendor: edmonsoft					
Product: read_more_\&_accordion					
Affected Version(s): * Up to (excluding) 3.2.7					
N/A	16-Oct-2023	7.2	The Read More & Accordion WordPress plugin before 3.2.7 unserializes user input provided via the settings, which could allow high-privilege users such as admin to perform PHP Object Injection when a suitable gadget is present. **CVE ID : CVE-2023-3392**	N/A	A-EDM-READ-231123/348
Vendor: edneville					
Product: please					
Affected Version(s): * Up to (including) 0.5.4					
N/A	20-Oct-2023	7.8	please (aka pleaser) through	https://gitlab.com/edneville/p	A-EDN-PLEA-231123/349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0.5.4 allows privilege escalation through the TIOCSTI and/or TIOCLINUX ioctl. (If both TIOCSTI and TIOCLINUX are disabled, this cannot be exploited.) **CVE ID : CVE-2023-46277**	lease/-/merge_requests/69#note_1594254575, https://github.com/rustsec/advisory-db/pull/1798	
Vendor: egeorjon					
Product: eg-attachments					
Affected Version(s): * Up to (including) 2.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Emmanuel GEORJON EG-Attachments plugin <= 2.1.3 versions. **CVE ID : CVE-2023-46070**	N/A	A-EGE-EG-A-231123/350
Vendor: Egroupware					
Product: egroupware					
Affected Version(s): 17.1.20190111					
Insufficiently Protected Credentials	26-Oct-2023	4.9	An issue was discovered in eGroupWare 17.1.20190111. An Improper Password Storage vulnerability affects the setup panel of under setup/manageheader.php, which allows authenticated remote attackers	N/A	A-EGR-EGRO-231123/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with administrator credentials to read a cleartext database password. **CVE ID : CVE-2023-38328**		
Vendor: Elastic					
Product: apm_server					
Affected Version(s): * Up to (excluding) 2.8					
N/A	26-Oct-2023	5.3	Secret token configuration is never applied when using ECK <2.8 with APM Server >=8.0. This could lead to anonymous requests to an APM Server being accepted and the data ingested into this APM deployment. **CVE ID : CVE-2023-31416**	https://www.elastic.co/community/security, https://discuss.elastic.co/t/elastic-cloud-on-kubernetes-eck-2-8-security-update/343854	A-ELA-APM_-231123/352
Product: elasticsearch					
Affected Version(s): * Up to (including) 7.17.12					
Uncontrolled Resource Consumption	26-Oct-2023	7.5	An issue has been identified with how Elasticsearch handled incoming requests on the HTTP layer. An unauthenticated user could force an Elasticsearch node to exit with an OutOfMemory error by sending a moderate number	https://discuss.elastic.co/t/elasticsearch-8-9-0-7-17-13-security-update/343616, https://www.elastic.co/community/security	A-ELA-ELAS-231123/353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of malformed HTTP requests. The issue was identified by Elastic Engineering and we have no indication that the issue is known or that it is being exploited in the wild. **CVE ID : CVE-2023-31418**		
Affected Version(s): From (including) 7.0.0 Up to (including) 7.17.12					
Insertion of Sensitive Information into Log File	26-Oct-2023	7.5	Elasticsearch generally filters out sensitive information and credentials before logging to the audit log. It was found that this filtering was not applied when requests to Elasticsearch use certain deprecated URIs for APIs. The impact of this flaw is that sensitive information such as passwords and tokens might be printed in cleartext in Elasticsearch audit logs. Note that audit logging is disabled by default and needs to be explicitly enabled and even when audit logging is enabled, request bodies that could	https://www.elastic.co/community/security, https://discuss.elastic.co/t/elasticsearch-8-9-2-and-7-17-13-security-update/342479	A-ELA-ELAS-231123/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain sensitive information are not printed to the audit log unless explicitly configured. **CVE ID : CVE-2023-31417**		
Out-of-bounds Write	26-Oct-2023	7.5	A flaw was discovered in Elasticsearch, affecting the _search API that allowed a specially crafted query string to cause a Stack Overflow and ultimately a Denial of Service. **CVE ID : CVE-2023-31419**	https://www.elastic.co/community/security, https://discuss.elastic.co/t/elasticsearch-8-9-1-7-17-13-security-update/343297	A-ELA-ELAS-231123/355
Affected Version(s): From (including) 8.0.0 Up to (including) 8.8.2					
Uncontrolled Resource Consumption	26-Oct-2023	7.5	An issue has been identified with how Elasticsearch handled incoming requests on the HTTP layer. An unauthenticated user could force an Elasticsearch node to exit with an OutOfMemory error by sending a moderate number of malformed HTTP requests. The issue was identified by Elastic Engineering and we have no indication that the	https://discuss.elastic.co/t/elasticsearch-8-9-0-7-17-13-security-update/343616, https://www.elastic.co/community/security	A-ELA-ELAS-231123/356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is known or that it is being exploited in the wild. **CVE ID : CVE-2023-31418**		
Affected Version(s): From (including) 8.0.0 Up to (including) 8.9.0					
Out-of-bounds Write	26-Oct-2023	7.5	A flaw was discovered in Elasticsearch, affecting the _search API that allowed a specially crafted query string to cause a Stack Overflow and ultimately a Denial of Service. **CVE ID : CVE-2023-31419**	https://www.elastic.co/community/security, https://discuss.elastic.co/t/elasticsearch-8-9-1-7-17-13-security-update/343297	A-ELA-ELAS-231123/357
Affected Version(s): From (including) 8.0.0 Up to (including) 8.9.1					
Insertion of Sensitive Information into Log File	26-Oct-2023	7.5	Elasticsearch generally filters out sensitive information and credentials before logging to the audit log. It was found that this filtering was not applied when requests to Elasticsearch use certain deprecated URIs for APIs. The impact of this flaw is that sensitive information such as passwords and	https://www.elastic.co/community/security, https://discuss.elastic.co/t/elasticsearch-8-9-2-and-7-17-13-security-update/342479	A-ELA-ELAS-231123/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tokens might be printed in cleartext in Elasticsearch audit logs. Note that audit logging is disabled by default and needs to be explicitly enabled and even when audit logging is enabled, request bodies that could contain sensitive information are not printed to the audit log unless explicitly configured. **CVE ID : CVE-2023-31417**		
Product: elastic_cloud_enterprise					
Affected Version(s): * Up to (including) 2.13.3					
Uncontrolled Resource Consumption	26-Oct-2023	7.5	An issue has been identified with how Elasticsearch handled incoming requests on the HTTP layer. An unauthenticated user could force an Elasticsearch node to exit with an OutOfMemory error by sending a moderate number of malformed HTTP requests. The issue was identified by Elastic Engineering and we have no indication that the issue is known or that it is being	https://discuss.elastic.co/t/elasticsearch-8-9-0-7-17-13-security-update/343616, https://www.elastic.co/community/security	A-ELA-ELAS-231123/359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploited in the wild. **CVE ID : CVE-2023-31418**		
Affected Version(s): 3.6.0					
Uncontrolled Resource Consumption	26-Oct-2023	7.5	An issue has been identified with how Elasticsearch handled incoming requests on the HTTP layer. An unauthenticated user could force an Elasticsearch node to exit with an OutOfMemory error by sending a moderate number of malformed HTTP requests. The issue was identified by Elastic Engineering and we have no indication that the issue is known or that it is being exploited in the wild. **CVE ID : CVE-2023-31418**	https://discuss.elastic.co/t/elasticsearch-8-9-0-7-17-13-security-update/343616, https://www.elastic.co/community/security	A-ELA-ELAS-231123/360
Product: elastic_cloud_on_kubernetes					
Affected Version(s): * Up to (excluding) 2.8					
N/A	26-Oct-2023	5.3	Secret token configuration is never applied when using ECK <2.8 with APM Server >=8.0. This could lead to anonymous requests to an APM	https://www.elastic.co/community/security, https://discuss.elastic.co/t/elastic-cloud-on-kubernetes-eck-	A-ELA-ELAS-231123/361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server being accepted and the data ingested into this APM deployment. **CVE ID : CVE-2023-31416**	2-8-security-update/343854	
Product: elastic_sharepoint_online_python_connector					
Affected Version(s): * Up to (excluding) 8.10.3.0					
N/A	26-Oct-2023	6.5	An issue was discovered when using Document Level Security and the SPO "Limited Access" functionality in Elastic Sharepoint Online Python Connector. If a user is assigned limited access permissions to an item on a Sharepoint site then that user would have read permissions to all content on the Sharepoint site through Elasticsearch. **CVE ID : CVE-2023-46666**	https://www.elastic.co/community/security, https://discuss.elastic.co/t/elastic-sharepoint-online-python-connector-v8-10-3-0-security-update/344732	A-ELA-ELAS-231123/362
Product: endpoint					
Affected Version(s): From (including) 7.9.0 Up to (including) 8.10.3					
Insertion of Sensitive Information into Log File	26-Oct-2023	9.1	If Elastic Endpoint (v7.9.0 - v8.10.3) is configured to use a non-default option in which the logging level is explicitly set to	https://www.elastic.co/community/security	A-ELA-ENDP-231123/363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			debug, and when Elastic Agent is simultaneously configured to collect and send those logs to Elasticsearch, then Elastic Agent API keys can be viewed in Elasticsearch in plaintext. These API keys could be used to write arbitrary data and read Elastic Endpoint user artifacts. **CVE ID : CVE-2023-46668**		
Product: fleet_server					
Affected Version(s): From (including) 8.10.0 Up to (excluding) 8.10.3					
Insertion of Sensitive Information into Log File	26-Oct-2023	8.1	An issue was discovered in Fleet Server >= v8.10.0 and < v8.10.3 where Agent enrolment tokens are being inserted into the Fleet Server's log file in plain text. These enrolment tokens could allow someone to enrol an agent into an agent policy, and potentially use that to retrieve other secrets in the policy including for Elasticsearch and third-party services.	https://www.elastic.co/community/security	A-ELA-FLEE-231123/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Alternatively a threat actor could potentially enrol agents to the clusters and send arbitrary events to Elasticsearch. **CVE ID : CVE-2023-46667**		
Product: kibana					
Affected Version(s): 8.10.0					
Insertion of Sensitive Information into Log File	26-Oct-2023	7.5	An issue was discovered by Elastic whereby sensitive information is recorded in Kibana logs in the event of an error. The issue impacts only Kibana version 8.10.0 when logging in the JSON layout or when the pattern layout is configured to log the %meta pattern. Elastic has released Kibana 8.10.1 which resolves this issue. The error object recorded in the log contains request information, which can include sensitive data, such as authentication credentials, cookies, authorization headers, query params, request	https://www.elastic.co/community/security, https://discuss.elastic.co/t/kibana-8-10-1-security-update/343287	A-ELA-KIBA-231123/365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			paths, and other metadata. Some examples of sensitive data which can be included in the logs are account credentials for kibana_system, kibana-metricbeat, or Kibana end-users. **CVE ID : CVE-2023-31422**		
Vendor: ellipticlabs					
Product: ai_virtual_presence_sensor					
Affected Version(s): * Up to (excluding) 3.1.50719.1					
Incorrect Default Permissions	25-Oct-2023	7.8	A vulnerability was reported in Elliptic Labs Virtual Lock Sensor for ThinkPad T14 Gen 3 that could allow an attacker with local access to execute code with elevated privileges. **CVE ID : CVE-2023-3112**	https://support.lenovo.com/us/en/product_security/LEN-128081	A-ELL-AI_V-231123/366
Product: virtual_lock_sensor					
Affected Version(s): * Up to (excluding) 3.1.50719.1					
Incorrect Default Permissions	25-Oct-2023	7.8	A vulnerability was reported in Elliptic Labs Virtual Lock Sensor for ThinkPad T14 Gen 3 that could allow an attacker with local access to execute code with elevated privileges.	https://support.lenovo.com/us/en/product_security/LEN-128081	A-ELL-VIRT-231123/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3112		
Vendor: engelsystem					
Product: engelsystem					
Affected Version(s): * Up to (excluding) 2023-09-18					
Insufficient Session Expiration	17-Oct-2023	2.8	Engelsystem is a shift planning system for chaos events. If a users' password is compromised and an attacker gained access to a users' account, i.e., logged in and obtained a session, an attackers' session is not terminated if the users' account password is reset. This vulnerability has been fixed in the commit `dbb089315ff3d`. Users are advised to update their installations. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45659**	https://github.com/engelsystem/engelsystem/security/advisories/GHSA-f6mm-3v2h-jm6x, https://github.com/engelsystem/engelsystem/commit/dbb089315ff3d8aabc11445e78fb50765208b27d	A-ENG-ENGE-231123/368
Server-Side Request Forgery (SSRF)	17-Oct-2023	2.3	Engelsystem is a shift planning system for chaos events. A Blind SSRF in the "Import schedule" functionality makes it possible to perform a port scan against the	https://github.com/engelsystem/engelsystem/commit/ee7d30b33935ea001705f438fec8ffd05734f295	A-ENG-ENGE-231123/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local environment. This vulnerability has been fixed in commit ee7d30b33. If a patch cannot be deployed, operators should ensure that no HTTP(s) services listen on localhost and/or systems only reachable from the host running the engelsystem software. If such services are necessary, they should utilize additional authentication. **CVE ID : CVE-2023-45152**		
Vendor: enghouse					
Product: qumu					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.0.63					
N/A	19-Oct-2023	7.8	A privilege escalation vulnerability exists within the Qumu Multicast Extension v2 before 2.0.63 for Windows. When a standard user triggers a repair of the software, a pop-up window opens with SYSTEM privileges. Standard users	N/A	A-ENG-QUMU-231123/370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may use this to gain arbitrary code execution as SYSTEM. **CVE ID : CVE-2023-45883**		
Vendor: enhancesoft					
Product: osticket					
Affected Version(s): 1.17.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	4.8	A stored cross-site scripting (XSS) vulnerability in the Admin panel in Enhancesoft osTicket v1.17.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Role Name parameter. **CVE ID : CVE-2023-27148**	N/A	A-ENH-OSTI-231123/371
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	4.8	A stored cross-site scripting (XSS) vulnerability in Enhancesoft osTicket v1.17.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Label input parameter when updating a custom list. **CVE ID : CVE-2023-27149**	N/A	A-ENH-OSTI-231123/372
Vendor: eprosima					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: fast_dds					
Affected Version(s): * Up to (excluding) 2.6.7					
Double Free	16-Oct-2023	7.5	Fast DDS is a C++ implementation of the DDS (Data Distribution Service) standard of the OMG (Object Management Group). In affected versions specific DATA submessages can be sent to a discovery locator which may trigger a free error. This can remotely crash any Fast-DDS process. The call to free() could potentially leave the pointer in the attackers control which could lead to a double free. This issue has been addressed in versions 2.12.0, 2.11.3, 2.10.3, and 2.6.7. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-42459**	https://github.com/eProsima/Fast-DDS/pull/3824, https://github.com/eProsima/Fast-DDS/security/advisories/GHSA-gq8g-fj58-22gm	A-EPR-FAST-231123/373
Affected Version(s): From (including) 2.10.0 Up to (excluding) 2.10.3					
Double Free	16-Oct-2023	7.5	Fast DDS is a C++ implementation of the DDS (Data	https://github.com/eProsima/Fast-	A-EPR-FAST-231123/374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Distribution Service) standard of the OMG (Object Management Group). In affected versions specific DATA submessages can be sent to a discovery locator which may trigger a free error. This can remotely crash any Fast-DDS process. The call to free() could potentially leave the pointer in the attackers control which could lead to a double free. This issue has been addressed in versions 2.12.0, 2.11.3, 2.10.3, and 2.6.7. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-42459**	DDS/pull/3824, https://github.com/eProsima/Fast-DDS/security/advisories/GHSA-gq8g-fj58-22gm	
Affected Version(s): From (including) 2.11.0 Up to (including) 2.11.1					
Double Free	16-Oct-2023	7.5	Fast DDS is a C++ implementation of the DDS (Data Distribution Service) standard of the OMG (Object Management Group). In affected versions specific	https://github.com/eProsima/Fast-DDS/pull/3824, https://github.com/eProsima/Fast-DDS/security/advisories/GHSA	A-EPR-FAST-231123/375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DATA submessages can be sent to a discovery locator which may trigger a free error. This can remotely crash any Fast-DDS process. The call to free() could potentially leave the pointer in the attackers control which could lead to a double free. This issue has been addressed in versions 2.12.0, 2.11.3, 2.10.3, and 2.6.7. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-42459**	-gq8g-fj58-22gm	
Vendor: eralion					
Product: animated_counters					
Affected Version(s): * Up to (including) 1.7					
N/A	27-Oct-2023	5.4	The Animated Counters plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 1.7 due to insufficient input sanitization	https://plugins.trac.wordpress.org/changeset/2984228/	A-ERA-ANIM-231123/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5774**		
Product: neon_text					
Affected Version(s): * Up to (including) 1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	5.4	The Neon text plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's neontext_box shortcode in all versions up to, and including, 1.1 due to insufficient input sanitization and output escaping on user supplied attributes (color). This makes it possible for authenticated attackers with contributor-level and above permissions to	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2984188%40neon-text&new=2984188%40neon-text&sfp_email=&sfph_mail=	A-ERA-NEON-231123/377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5817**		
Vendor: ericteubert					
Product: archivist_-_custom_archive_templates					
Affected Version(s): * Up to (including) 1.7.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Eric Teubert Archivist – Custom Archive Templates plugin <= 1.7.5 versions. **CVE ID : CVE-2023-46194**	N/A	A-ERI-ARCH-231123/378
Vendor: esst					
Product: esst_monitoring					
Affected Version(s): * Up to (including) 2.147.1					
Improper Control of Generation of Code ('Code Injection')	17-Oct-2023	9.8	eSST Monitoring v2.147.1 was discovered to contain a remote code execution (RCE) vulnerability via the Gii code generator component. **CVE ID : CVE-2023-41630**	N/A	A-ESS-ESST-231123/379
Unrestricted Upload of File with Dangerous Type	17-Oct-2023	8.8	eSST Monitoring v2.147.1 was discovered to contain a remote code execution	N/A	A-ESS-ESST-231123/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(RCE) vulnerability via the file upload function. **CVE ID : CVE-2023-41631**		
N/A	17-Oct-2023	7.5	A lack of input sanitizing in the file download feature of eSST Monitoring v2.147.1 allows attackers to execute a path traversal. **CVE ID : CVE-2023-41629**	N/A	A-ESS-ESST-231123/381
Vendor: ethereum					
Product: go_ethereum					
Affected Version(s): * Up to (including) 1.13.4					
N/A	18-Oct-2023	7.5	Geth (aka go-ethereum) through 1.13.4, when --http --graphql is used, allows remote attackers to cause a denial of service (memory consumption and daemon hang) via a crafted GraphQL query. NOTE: the vendor's position is that the "graphql endpoint [is not] designed to withstand attacks by hostile clients, nor handle huge amounts of clients/traffic. **CVE ID : CVE-2023-42319**	https://geth.ethereum.org/docs/fundamentals/security	A-ETH-GO_E-231123/382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: ethyca					
Product: fides					
Affected Version(s): * Up to (excluding) 2.22.1					
Server-Side Request Forgery (SSRF)	25-Oct-2023	7.2	Fides is an open-source privacy engineering platform for managing the fulfillment of data privacy requests in runtime environments, and the enforcement of privacy regulations in code. The Fides web application allows a custom integration to be uploaded as a ZIP file containing configuration and dataset definitions in YAML format. It was discovered that specially crafted YAML dataset and config files allow a malicious user to perform arbitrary requests to internal systems and exfiltrate data outside the environment (also known as a Server-Side Request Forgery). The application does not perform proper validation to block attempts to connect to internal	https://github.com/ethyca/fides/commit/cd344d016b1441662a61d0759e7913e8228ed1ee	A-ETH-FIDE-231123/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(including localhost) resources. The vulnerability has been patched in Fides version `2.22.1`. **CVE ID : CVE-2023-46124**		
Incorrect Authorization	25-Oct-2023	6.5	Fides is an open-source privacy engineering platform for managing the fulfillment of data privacy requests in a runtime environment, and the enforcement of privacy regulations in code. The Fides webserver API allows users to retrieve its configuration using the `GET api/v1/config` endpoint. The configuration data is filtered to suppress most sensitive configuration information before it is returned to the user, but even the filtered data contains information about the internals and the backend infrastructure, such as various	https://github.com/ethyca/fides/commit/c9f3a620a4b4c1916e0941cb5624dcd636f06d06	A-ETH-FIDE-231123/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			settings, servers' addresses and ports and database username. This information is useful for administrative users as well as attackers, thus it should not be revealed to low-privileged users. This vulnerability allows Admin UI users with roles lower than the owner role e.g. the viewer role to retrieve the config information using the API. The vulnerability has been patched in Fides version `2.22.1`. **CVE ID : CVE-2023-46125**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	Fides is an open-source privacy engineering platform for managing the fulfillment of data privacy requests in runtime environments, helping enforce privacy regulations in code. The Fides web application allows users to edit consent and privacy notices	https://github.com/ethyca/fides/commit/3231d19699f9c895c986f6a967a64d882769c506	A-ETH-FIDE-231123/385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such as cookie banners. The vulnerability makes it possible to craft a payload in the privacy policy URL which triggers JavaScript execution when the privacy notice is served by an integrated website. The domain scope of the executed JavaScript is that of the integrated website. Exploitation is limited to Admin UI users with the contributor role or higher. The vulnerability has been patched in Fides version `2.22.1`. **CVE ID : CVE-2023-46126**		
Vendor: eupago					
Product: eupago_gateway_woocommerce					
Affected Version(s): * Up to (including) 3.1.9					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in euPago Eupago Gateway For Woocommerce plugin <= 3.1.9 versions. **CVE ID : CVE-2023-45638**	N/A	A-EUP-EUPA-231123/386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: evo					
Product: evolution_cms					
Affected Version(s): 3.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2023	6.1	Cross-site scripting (XSS) vulnerability in evolution evo v.3.2.3 allows a local attacker to execute arbitrary code via a crafted payload injected uid parameter. **CVE ID : CVE-2023-43341**	N/A	A-EVO-EVOL-231123/387
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2023	5.2	Cross-site scripting (XSS) vulnerability in evolution v.3.2.3 allows a local attacker to execute arbitrary code via a crafted payload injected into the cmsadmin, cmsadminemail, cmspassword and cmspasswordconfim parameters **CVE ID : CVE-2023-43340**	N/A	A-EVO-EVOL-231123/388
Vendor: expense_management_system_project					
Product: expense_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	17-Oct-2023	7.8	An issue in Expense Management System v.1.0 allows a local attacker to execute arbitrary code via a crafted file uploaded to the	N/A	A-EXP-EXPE-231123/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sign-up.php component. **CVE ID : CVE-2023-44824**		
Vendor: extendwings					
Product: opcache_dashboard					
Affected Version(s): * Up to (including) 0.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Daisuke Takahashi(Extend Wings) OPcache Dashboard plugin <= 0.3.1 versions. **CVE ID : CVE-2023-45064**	N/A	A-EXT-OPCA-231123/390
Vendor: ezoic					
Product: ampedsense					
Affected Version(s): * Up to (including) 4.68					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Ezoic AmpedSense – AdSense Split Tester plugin <= 4.68 versions. **CVE ID : CVE-2023-25476**	N/A	A-EZO-AMPE-231123/391
Vendor: F5					
Product: big-ip_access_policy_manager					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Authentication Bypass Using an Alternate	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication,	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Path or Channel			allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/394
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/397
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/399
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
Authentication Bypass Using an Alternate	26-Oct-2023	9.8	Undisclosed requests may bypass	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Path or Channel			configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Product: big-ip_advanced_firewall_manager					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/402
Improper Neutralization of Special Elements used in an SQL Command	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46747		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/405
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/407
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/408
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/410
Improper Neutralization of	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists	https://my.f5.com/manage/s/	A-F5-BIG--231123/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	article/K00013 7365	
Product: big-ip_advanced_web_application_firewall					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Authentica tion Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system	https://my.f5.com/manage/s/article/K00013 7353	A-F5-BIG--231123/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/413
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentication Bypass Using an Alternate	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Path or Channel			authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands.	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/416
Improper Neutralization of Special Elements used in an SQL Command	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/419
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/421
Product: big-ip_analytics					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/422
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands.	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/424
Improper Neutralization of Special Elements used in an SQL Command	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/427
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/429
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/430
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Product: big-ip_application_acceleration_manager					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/432
Improper Neutralization of	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists	https://my.f5.com/manage/s/	A-F5-BIG--231123/433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	article/K00013 7365	
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentica tion Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note:	https://my.f5.com/manage/s/article/K00013 7353	A-F5-BIG--231123/434

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-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/435
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
Authentication Bypass Using an Alternate	26-Oct-2023	9.8	Undisclosed requests may bypass configuration	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Path or Channel			utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/438
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/441
Product: big-ip_application_security_manager					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/443
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentication Bypass Using an	26-Oct-2023	9.8	Undisclosed requests may bypass configuration	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Alternate Path or Channel			utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/446
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/449
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/451
Product: big-ip_application_visibility_and_reporting					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Authentication Bypass	26-Oct-2023	9.8		https://my.f5.com/manage/s/	A-F5-BIG--231123/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Using an Alternate Path or Channel			Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	article/K00013 7353	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands.	https://my.f5.com/manage/s/article/K00013 7365	A-F5-BIG--231123/453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/454
Improper Neutralization of Special Elements used in an SQL	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/457
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/459
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/460
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands.	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Product: big-ip_automation_toolchain					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/462
Improper Neutralization of Special Elements used in an SQL	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/465
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/467
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/468
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/470
Improper Neutralization of Special Elements	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Product: big-ip_carrier-grade_nat					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/473
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46748		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/476
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/478
Improper Neutralization of	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists	https://my.f5.com/manage/s/	A-F5-BIG--231123/479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	article/K00013 7365	
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
Authentica tion Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have	https://my.f5.c om/manage/s/ article/K00013 7353	A-F5-BIG-- 231123/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/481
Product: big-ip_container_ingress_services					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46748		
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/484
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/486
Improper Neutralization of Special Elements	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/489
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/491
Product: big-ip_ddos_hybrid_defender					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/492
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands.	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/494
Improper Neutralization of Special Elements used in an SQL Command	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46747		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/497
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/499
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
Authentication Bypass	26-Oct-2023	9.8	Undisclosed requests may bypass	https://my.f5.com/manage/s/	A-F5-BIG--231123/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Using an Alternate Path or Channel			configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	article/K00013 7353	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End	https://my.f5.com/manage/s/article/K00013 7365	A-F5-BIG--231123/501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Product: big-ip_domain_name_system					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/502
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/505
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/507
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					
Authentication Bypass Using an Alternate	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication,	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Path or Channel			allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46748		
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/510
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Product: big-ip_fraud_protection_services					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/512
Improper Neutralization of Special	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP	https://my.f5.com/manage/s/	A-F5-BIG--231123/513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	article/K00013 7365	
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentica tion Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of	https://my.f5.com/manage/s/article/K00013 7353	A-F5-BIG--231123/514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/515
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/517
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/518
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands.	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/520
Improper Neutralization of Special Elements used in an SQL Command	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Product: big-ip_global_traffic_manager					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/523
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/525
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/526
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands.	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/528
Improper Neutralization of Special Elements used in an SQL Command	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46747		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/531
Product: big-ip_link_controller					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/533
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentication	26-Oct-2023	9.8	Undisclosed requests may	https://my.f5.com/manage/s/	A-F5-BIG--231123/534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bypass Using an Alternate Path or Channel			bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	article/K00013 7353	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which	https://my.f5.com/manage/s/article/K00013 7365	A-F5-BIG--231123/535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/536
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/539
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/541
Product: big-ip_local_traffic_manager					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Authentication Bypass Using an Alternate	26-Oct-2023	9.8	Undisclosed requests may bypass	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Path or Channel			configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/544
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46747		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/547
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/549
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--231123/550
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands.	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--231123/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Product: big-ip_policy_enforcement_manager					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--241123/552
Improper Neutralization of Special Elements used in an SQL	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--241123/553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--241123/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--241123/555
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--241123/556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--241123/557
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--241123/558
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands.	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--241123/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--241123/560
Improper Neutralization of Special Elements used in an SQL Command	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--241123/561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Product: big-ip_ssl_orchestrator					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--241123/562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--241123/563
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--241123/564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--241123/565
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--241123/566
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands.	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--241123/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--241123/568
Improper Neutralization of Special Elements used in an SQL Command	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--241123/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--241123/570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46747		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--241123/571
Product: big-ip_webaccelerator					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--241123/572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--241123/573
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentication	26-Oct-2023	9.8	Undisclosed requests may	https://my.f5.com/manage/s/	A-F5-BIG--241123/574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bypass Using an Alternate Path or Channel			bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	article/K00013 7353	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which	https://my.f5.com/manage/s/article/K00013 7365	A-F5-BIG--241123/575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--241123/576
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--241123/577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--241123/578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--241123/579
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--241123/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--241123/581
Product: big-ip_websafe					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Authentication Bypass Using an Alternate	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--241123/582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Path or Channel			authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--241123/583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--241123/584
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--241123/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**		
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--241123/586
Improper Neutralizat	26-Oct-2023	8.8	An authenticated SQL injection	https://my.f5.com/manage/s/	A-F5-BIG--241123/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	article/K00013 7365	
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					
Authentica tion Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions	https://my.f5.com/manage/s/article/K00013 7353	A-F5-BIG--241123/588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46748**	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--241123/589
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
Authentication Bypass Using an Alternate Path or Channel	26-Oct-2023	9.8	Undisclosed requests may bypass configuration utility authentication, allowing an attacker with	https://my.f5.com/manage/s/article/K000137353	A-F5-BIG--241123/590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated **CVE ID : CVE-2023-46747**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	An authenticated SQL injection vulnerability exists in the BIG-IP Configuration utility which may allow an authenticated attacker with network access to the Configuration utility through the BIG-IP management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	https://my.f5.com/manage/s/article/K000137365	A-F5-BIG--241123/591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46748		
Vendor: Facebook					
Product: react-devtools					
Affected Version(s): * Up to (excluding) 4.28.4					
N/A	19-Oct-2023	6.5	The React Developer Tools extension registers a message listener with window.addEventListener('message', <listener>) in a content script that is accessible to any webpage that is active in the browser. Within the listener is code that requests a URL derived from the received message via fetch(). The URL is not validated or sanitised before it is fetched, thus allowing a malicious web page to arbitrarily fetch URL's via the victim's browser. **CVE ID : CVE-2023-5654**	https://gist.github.com/CalumHutton/1fb89b64409570a43f89d1fd3274b231	A-FAC-REAC-241123/592
Vendor: fareharbor					
Product: fareharbor					
Affected Version(s): * Up to (including) 3.6.7					
Improper Neutralization of Special	30-Oct-2023	5.4	The FareHarbor plugin for WordPress is vulnerable to	https://plugins.trac.wordpress.org/browser/fareharbor/tags/	A-FAR-FARE-241123/593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			Stored Cross-Site Scripting via shortcodes in versions up to, and including, 3.6.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5252**	3.6.7/fareharbor.php#L287	
Vendor: fastlinemedia					
Product: assistant					
Affected Version(s): * Up to (excluding) 1.4.4					
N/A	26-Oct-2023	8.8	The Assistant WordPress plugin before 1.4.4 does not validate a parameter before making a request to it via wp_remote_get(), which could allow users with a role as low as Editor to perform SSRF attacks	N/A	A-FAS-ASSI-241123/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5798		
Vendor: fastwpspeed					
Product: fast_wp_speed					
Affected Version(s): * Up to (including) 1.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Fastwpspeed Fast WP Speed plugin <= 1.0.0 versions. **CVE ID : CVE-2023-45770**	N/A	A-FAS-FAST-241123/595
Vendor: feed_statistics_project					
Product: feed_statistics					
Affected Version(s): * Up to (including) 4.1					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Christopher Finke Feed Statistics plugin <= 4.1 versions. **CVE ID : CVE-2023-45605**	N/A	A-FEE-FEED-241123/596
Vendor: Ffmpeg					
Product: ffmpeg					
Affected Version(s): * Up to (excluding) 2023-10-17					
Out-of-bounds Read	27-Oct-2023	5.5	FFmpeg prior to commit bf814 was discovered to contain an out of bounds read via the dist->alphabet_size variable in the read_vlc_prefix() function.	https://github.com/FFmpeg/FFmpeg/commit/bf814387f42e9b0dea9d75c03db4723c88e7d962, https://patchwork.ffmpeg.org/project/ffmpeg/	A-FFM-FFMP-241123/597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46407	patch/20231015004924.597746-1-leo.izen%40gmail.com/	
Vendor: firecask					
Product: whatsapp_share_button					
Affected Version(s): * Up to (including) 1.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	The WhatsApp Share Button plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'whatsapp' shortcode in all versions up to, and including, 1.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5668**	https://plugins.trac.wordpress.org/browser/whatsapp/tags/1.0.1/class-frontend.php#L46	A-FIR-WHAT-241123/598
Vendor: fit2cloud					
Product: cloudexplorer_lite					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.4.1					
Improper Authentication	30-Oct-2023	9.8	CloudExplorer Lite is an open source, lightweight cloud management platform. Prior to version 1.4.1, the gateway filter of CloudExplorer Lite uses a controller with path starting with `matching/API/`, which can cause a permission bypass. Version 1.4.1 contains a patch for this issue. **CVE ID : CVE-2023-44397**	N/A	A-FIT-CLOU-241123/599
Product: jumpserver					
Affected Version(s): * Up to (excluding) 3.8.0					
Improper Restriction of Excessive Authentication Attempts	25-Oct-2023	5.3	jumpserver is an open source bastion machine, professional operation and maintenance security audit system that complies with 4A specifications. A flaw in the Core API allows attackers to bypass password brute-force protections by spoofing arbitrary IP addresses. By exploiting this vulnerability,	https://github.com/jumpserver/jumpserver/security/advisories/GHSA-hvw4-766m-p89f	A-FIT-JUMP-241123/600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers can effectively make unlimited password attempts by altering their apparent IP address for each request. This vulnerability has been patched in version 3.8.0. **CVE ID : CVE-2023-46123**		
Vendor: fla-shop					
Product: html5_maps					
Affected Version(s): * Up to (including) 1.7.1.4					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Fla-shop.Com HTML5 Maps plugin <= 1.7.1.4 versions. **CVE ID : CVE-2023-45650**	N/A	A-FLA-HTML-241123/601
Vendor: flowpaper					
Product: flowpaper					
Affected Version(s): * Up to (including) 2.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	The flowpaper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'flipbook' shortcode in versions up to, and including, 2.0.3 due to insufficient input sanitization and output	https://plugins.trac.wordpress.org/changeset/2966821/flowpaper-lite-pdf-flipbook, https://plugins.trac.wordpress.org/browser/flowpaper-lite-pdf-flipbook/trunk/flowpaper.php?	A-FLO-FLOW-241123/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5200**	rev=2959754#L395	
Vendor: fluisity					
Product: fluisity					
Affected Version(s): * Up to (excluding) 2023-10-24					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2023	5.4	A vulnerability was found in flusity CMS and classified as problematic. This issue affects the function loadCustomBlocCreateForm of the file /core/tools/custommblock.php of the component Dashboard. The manipulation of the argument custombloc k_place leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may	https://github.com/flusity/flusity-CMS/commit/81252bc764e1de2422e79e36194bba1289e7a0a5	A-FLU-FLUI-241123/603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The patch is named 81252bc764e1de2422e79e36194bba1289e7a0a5. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-243599. **CVE ID : CVE-2023-5793**		
Vendor: flusity					
Product: cms					
Affected Version(s): * Up to (including) 2.304					
N/A	27-Oct-2023	8.8	A vulnerability has been found in flusity CMS and classified as critical. Affected by this vulnerability is the function handleFileUpload of the file core/tools/upload.php. The manipulation of the argument uploaded_file leads to unrestricted upload. The attack can be launched remotely. The	N/A	A-FLU-CMS-241123/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The associated identifier of this vulnerability is VDB-243643. **CVE ID : CVE-2023-5812**		
Product: flusity					
Affected Version(s): * Up to (excluding) 2023-10-24					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	4.8	A vulnerability, which was classified as problematic, has been found in flusity CMS. This issue affects the function loadPostAddForm of the file core/tools/posts.php. The manipulation of the argument edit_post_id leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product takes the approach of rolling	https://github.com/flusity/flusity-CMS/commit/6943991c62ed87c7a57989a0cb7077316127def8	A-FLU-FLUS-241123/605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The identifier of the patch is 6943991c62ed87c7a57989a0cb7077316127def8. It is recommended to apply a patch to fix this issue. The identifier VDB-243641 was assigned to this vulnerability. **CVE ID : CVE-2023-5810**		
Vendor: flyte					
Product: flyteadmin					
Affected Version(s): * Up to (excluding) 1.1.124					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-Oct-2023	8.8	FlyteAdmin is the control plane for Flyte responsible for managing entities and administering workflow executions. Prior to version 1.1.124, list endpoints on FlyteAdmin have a SQL vulnerability where a malicious user can send a REST request with custom SQL statements as list	https://github.com/flyteorg/flyteadmin/commit/b3177ef70f068e908140b8a4a9913dfa74f289fd	A-FLY-FLYT-241123/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			filters. The attacker needs to have access to the FlyteAdmin installation, typically either behind a VPN or authentication. Version 1.1.124 contains a patch for this issue. **CVE ID : CVE-2023-41891**		
Vendor: formforall					
Product: formforall					
Affected Version(s): * Up to (including) 1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	The Contact form Form For All plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'formforall' shortcode in versions up to, and including, 1.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever	N/A	A-FOR-FORM-241123/607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a user accesses an injected page. **CVE ID : CVE-2023-5337**		
Vendor: Fortinet					
Product: fortianalyzer					
Affected Version(s): 7.4.0					
Server-Side Request Forgery (SSRF)	20-Oct-2023	6.5	A server-side request forgery vulnerability [CWE-918] in Fortinet FortiAnalyzer version 7.4.0, version 7.2.0 through 7.2.3 and before 7.0.8 and FortiManager version 7.4.0, version 7.2.0 through 7.2.3 and before 7.0.8 allows a remote attacker with low privileges to view sensitive data from internal servers or perform a local port scan via a crafted HTTP request. **CVE ID : CVE-2023-44256**	https://fortiguard.com/psirt/FG-IR-19-039	A-FOR-FORT-241123/608
Affected Version(s): From (including) 6.4.8 Up to (including) 6.4.13					
Server-Side Request Forgery (SSRF)	20-Oct-2023	6.5	A server-side request forgery vulnerability [CWE-918] in Fortinet FortiAnalyzer version 7.4.0, version 7.2.0	https://fortiguard.com/psirt/FG-IR-19-039	A-FOR-FORT-241123/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 7.2.3 and before 7.0.8 and FortiManager version 7.4.0, version 7.2.0 through 7.2.3 and before 7.0.8 allows a remote attacker with low privileges to view sensitive data from internal servers or perform a local port scan via a crafted HTTP request. **CVE ID : CVE-2023-44256**		
Affected Version(s): From (including) 7.0.2 Up to (including) 7.0.8					
Server-Side Request Forgery (SSRF)	20-Oct-2023	6.5	A server-side request forgery vulnerability [CWE-918] in Fortinet FortiAnalyzer version 7.4.0, version 7.2.0 through 7.2.3 and before 7.0.8 and FortiManager version 7.4.0, version 7.2.0 through 7.2.3 and before 7.0.8 allows a remote attacker with low privileges to view sensitive data from internal servers or perform a local port scan via a crafted HTTP request.	https://fortiguard.com/psirt/FG-IR-19-039	A-FOR-FORT-241123/610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-44256		
Affected Version(s): From (including) 7.2.0 Up to (including) 7.2.3					
Server-Side Request Forgery (SSRF)	20-Oct-2023	6.5	A server-side request forgery vulnerability [CWE-918] in Fortinet FortiAnalyzer version 7.4.0, version 7.2.0 through 7.2.3 and before 7.0.8 and FortiManager version 7.4.0, version 7.2.0 through 7.2.3 and before 7.0.8 allows a remote attacker with low privileges to view sensitive data from internal servers or perform a local port scan via a crafted HTTP request. **CVE ID : CVE-2023-44256**	https://fortiguard.com/psirt/FG-IR-19-039	A-FOR-FORT-241123/611
Product: fortimanager					
Affected Version(s): 7.4.0					
Server-Side Request Forgery (SSRF)	20-Oct-2023	6.5	A server-side request forgery vulnerability [CWE-918] in Fortinet FortiAnalyzer version 7.4.0, version 7.2.0 through 7.2.3 and before 7.0.8 and FortiManager version 7.4.0,	https://fortiguard.com/psirt/FG-IR-19-039	A-FOR-FORT-241123/612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 7.2.0 through 7.2.3 and before 7.0.8 allows a remote attacker with low privileges to view sensitive data from internal servers or perform a local port scan via a crafted HTTP request. **CVE ID : CVE-2023-44256**		
Affected Version(s): From (including) 7.2.0 Up to (including) 7.2.3					
Server-Side Request Forgery (SSRF)	20-Oct-2023	6.5	A server-side request forgery vulnerability [CWE-918] in Fortinet FortiAnalyzer version 7.4.0, version 7.2.0 through 7.2.3 and before 7.0.8 and FortiManager version 7.4.0, version 7.2.0 through 7.2.3 and before 7.0.8 allows a remote attacker with low privileges to view sensitive data from internal servers or perform a local port scan via a crafted HTTP request. **CVE ID : CVE-2023-44256**	https://fortiguard.com/psirt/FG-IR-19-039	A-FOR-FORT-241123/613
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	20-Oct-2023	6.5	A server-side request forgery vulnerability [CWE-918] in Fortinet FortiAnalyzer version 7.4.0, version 7.2.0 through 7.2.3 and before 7.0.8 and FortiManager version 7.4.0, version 7.2.0 through 7.2.3 and before 7.0.8 allows a remote attacker with low privileges to view sensitive data from internal servers or perform a local port scan via a crafted HTTP request. **CVE ID : CVE-2023-44256**	https://fortiguard.com/psirt/FG-IR-19-039	A-FOR-FORT-241123/614
Vendor: fossies					
Product: catdoc					
Affected Version(s): 0.95					
NULL Pointer Dereference	26-Oct-2023	7.5	Catdoc v0.95 was discovered to contain a NULL pointer dereference via the component xls2csv at src/xlsparse.c. **CVE ID : CVE-2023-46345**	N/A	A-FOS-CATD-241123/615
Vendor: fotomoto					
Product: fotomoto					
Affected Version(s): * Up to (including) 1.2.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Fotomoto plugin <= 1.2.8 versions. **CVE ID : CVE-2023-45007**	N/A	A-FOT-FOTO-241123/616
Vendor: frappe					
Product: frappe					
Affected Version(s): * Up to (excluding) 14.49.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	5.4	Frappe is a full-stack web application framework that uses Python and MariaDB on the server side and an integrated client side library. A malicious Frappe user with desk access could create documents containing HTML payloads allowing HTML Injection. This vulnerability has been patched in version 14.49.0. **CVE ID : CVE-2023-46127**	https://github.com/frappe/frappe/commit/3dc5d2fcc7561dde181ba953009fe6e39d64e900, https://github.com/frappe/frappe/security/advisories/GHSA-j2w9-8xrr-7g98	A-FRA-FRAP-241123/617
Vendor: free5gc					
Product: udm					
Affected Version(s): * Up to (excluding) 1.2.0					
Improper Verification of Cryptograp	23-Oct-2023	7.5	pkg/suci/suci.go in free5GC udm before 1.2.0, when Go before 1.19 is used, allows an	https://github.com/free5gc/udm/pull/20	A-FRE-UDM-241123/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
hic Signature			Invalid Curve Attack because it may compute a shared secret via an uncompressed public key that has not been validated. An attacker can send arbitrary SUCIs to the UDM, which tries to decrypt them via both its private key and the attacker's public key. **CVE ID : CVE-2023-46324**		
Vendor: freelancer-coder					
Product: wordpress_simple_html_sitemap					
Affected Version(s): * Up to (including) 2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Ashish Ajani WordPress Simple HTML Sitemap plugin <= 2.1 versions. **CVE ID : CVE-2023-45067**	N/A	A-FRE-WORD-241123/619
Vendor: frostming					
Product: pdm					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.10.0					
N/A	20-Oct-2023	7.8	pdm is a Python package and dependency manager supporting the latest PEP	https://github.com/pdm-project/pdm/commit/6853e2642dfa281d4a9958fbc6c95b7e3	A-FRO-PDM-241123/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			standards. It's possible to craft a malicious `pdm.lock` file that could allow e.g. an insider or a malicious open source project to appear to depend on a trusted PyPI project, but actually install another project. A project `foo` can be targeted by creating the project `foo-2` and uploading the file `foo-2-2.tar.gz` to pypi.org. PyPI will see this as project `foo-2` version `2`, while PDM will see this as project `foo` version `2-2`. The version must only be `parseable as a version` and the filename must be a prefix of the project name, but it's not verified to match the version being installed. Version `2-2` is also not a valid normalized version per PEP 440. Matching the project name exactly (not just prefix) would fix the issue. When installing	2d84831, https://github.com/pdm-project/pdm/security/advisories/GHSA-j44v-mmf2-xvm9	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dependencies with PDM, what's actually installed could differ from what's listed in `pyproject.toml` (including arbitrary code execution on install). It could also be used for downgrade attacks by only changing the version. This issue has been addressed in commit `6853e2642df` which is included in release version `2.9.4`. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45805**		
Product: unearth					
Affected Version(s): * Up to (excluding) 0.11.2					
N/A	20-Oct-2023	7.8	pdm is a Python package and dependency manager supporting the latest PEP standards. It's possible to craft a malicious `pdm.lock` file that could allow e.g. an insider or a malicious open	https://github.com/pdm-project/pdm/commit/6853e2642dfa281d4a9958fbc6c95b7e32d84831, https://github.com/pdm-project/pdm/security/advisorie	A-FRO-UNEA-241123/621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			source project to appear to depend on a trusted PyPI project, but actually install another project. A project `foo` can be targeted by creating the project `foo-2` and uploading the file `foo-2-2.tar.gz` to pypi.org. PyPI will see this as project `foo-2` version `2`, while PDM will see this as project `foo` version `2-2`. The version must only be `parseable as a version` and the filename must be a prefix of the project name, but it's not verified to match the version being installed. Version `2-2` is also not a valid normalized version per PEP 440. Matching the project name exactly (not just prefix) would fix the issue. When installing dependencies with PDM, what's actually installed could differ from what's listed in `pyproject.toml` (including	s/GHSA-j44v-mmf2-xvm9	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution on install). It could also be used for downgrade attacks by only changing the version. This issue has been addressed in commit `6853e2642df` which is included in release version `2.9.4`. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45805**		
Vendor: frrouting					
Product: frrouting					
Affected Version(s): * Up to (including) 9.0.1					
N/A	26-Oct-2023	7.5	An issue was discovered in FRRouting FRR through 9.0.1. It mishandles malformed MP_REACH_NLRI data, leading to a crash. **CVE ID : CVE-2023-46752**	https://github.com/FRRouting/frr/pull/14645/commits/b08afc81c60607a4f736f418f2e3eb06087f1a35	A-FRR-FRRO-241123/622
N/A	26-Oct-2023	7.5	An issue was discovered in FRRouting FRR through 9.0.1. A crash can occur for a crafted BGP UPDATE message	https://github.com/FRRouting/frr/pull/14645/commits/d8482bf011cb2b173	A-FRR-FRRO-241123/623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without mandatory attributes, e.g., one with only an unknown transit attribute. **CVE ID : CVE-2023-46753**	e85b65b4bf3d5061250cdb9	
Vendor: funnelforms					
Product: funnelforms					
Affected Version(s): * Up to (excluding) 3.4					
N/A	16-Oct-2023	6.1	The Interactive Contact Form and Multi Step Form Builder WordPress plugin before 3.4 does not sanitise and escape some parameters, which could allow unauthenticated users to perform Cross-Site Scripting attacks **CVE ID : CVE-2023-4950**	N/A	A-FUN-FUNN-241123/624
Vendor: g5theme					
Product: grid-plus					
Affected Version(s): * Up to (including) 1.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in G5Theme Grid Plus – Unlimited grid plugin <= 1.3.2 versions. **CVE ID : CVE-2023-46209**	N/A	A-G5T-GRID-241123/625
Product: grid_plus					
Affected Version(s): * Up to (including) 1.3.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	30-Oct-2023	8.8	The Grid Plus plugin for WordPress is vulnerable to Local File Inclusion in versions up to, and including, 1.3.2 via a shortcode attribute. This allows subscriber-level, and above, attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where PHP files with arbitrary content can be uploaded and included. This is limited to .php files. **CVE ID : CVE-2023-5250**	N/A	A-G5T-GRID-241123/626
Missing Authorization	30-Oct-2023	5.4	The Grid Plus plugin for WordPress is vulnerable to unauthorized modification of data and loss of data due to a missing capability check on the	N/A	A-G5T-GRID-241123/627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'grid_plus_save_layout_callback' and 'grid_plus_delete_callback' functions in versions up to, and including, 1.3.2. This makes it possible for authenticated attackers with subscriber privileges or above, to add, update or delete grid layout. **CVE ID : CVE-2023-5251**		
Vendor: galaxyweblinks					
Product: video_playlist_for_youtube					
Affected Version(s): * Up to (including) 6.0					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Galaxy Weblinks Video Playlist For YouTube plugin <= 6.0 versions. **CVE ID : CVE-2023-45653**	N/A	A-GAL-VIDE-241123/628
Vendor: gamipress					
Product: gamipress					
Affected Version(s): * Up to (including) 2.5.7					
Improper Neutralization of Special Elements used in an SQL Command	31-Oct-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in GamiPress gamipress allows SQL Injection.This	N/A	A-GAM-GAMI-241123/629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			issue affects GamiPress: from n/a through 2.5.7. **CVE ID : CVE-2023-24000**		
Vendor: Geeklog					
Product: geeklog					
Affected Version(s): 2.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Oct-2023	4.8	Cross Site Scripting (XSS) vulnerability in Geeklog-Core geeklog v.2.2.2 allows a remote attacker to execute arbitrary code via a crafted payload to the grp_desc parameter of the admin/group.php component. **CVE ID : CVE-2023-46058**	N/A	A-GEE-GEEK-241123/630
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Oct-2023	4.8	Cross Site Scripting (XSS) vulnerability in Geeklog-Core geeklog v.2.2.2 allows a remote attacker to execute arbitrary code via a crafted payload to the Service, and website URL to Ping parameters of the admin/trackback.php component. **CVE ID : CVE-2023-46059**	N/A	A-GEE-GEEK-241123/631
Vendor: Geoserver					
Product: geowebcache					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.15.1					
Direct Request ('Forced Browsing')	26-Oct-2023	8.8	A vulnerability was found in GeoServer GeoWebCache up to 1.15.1. It has been declared as problematic. This vulnerability affects unknown code of the file /geoserver/gwc/rest.html. The manipulation leads to direct request. 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-243592. **CVE ID : CVE-2023-5786**	N/A	A-GEO-GEOW-241123/632
Vendor: Get-simple					
Product: getsimplecms					
Affected Version(s): 3.4.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Oct-2023	5.4	Cross Site Scripting vulnerability in GetSimpleCMS v.3.4.0a allows a remote attacker to execute arbitrary code via the a crafted payload to the components.php function. **CVE ID : CVE-2023-46040**	N/A	A-GET-GETS-241123/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 3.4.0a					
N/A	19-Oct-2023	9.8	An issue in GetSimpleCMS v.3.4.0a allows a remote attacker to execute arbitrary code via a crafted payload to the phpinfo(). **CVE ID : CVE-2023-46042**	N/A	A-GET-GETS-241123/634
Vendor: getbutterfly					
Product: youtube_playlist_player					
Affected Version(s): * Up to (excluding) 4.6.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Ciprian Popescu YouTube Playlist Player plugin <= 4.6.7 versions. **CVE ID : CVE-2023-45049**	N/A	A-GET-YOUT-241123/635
Vendor: getlasso					
Product: simple_urls					
Affected Version(s): * Up to (including) 120					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Lasso Simple URLs plugin <= 120 versions. **CVE ID : CVE-2023-45606**	N/A	A-GET-SIMP-241123/636
Vendor: gettimely					
Product: timely_booking_button					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Timely - Appointment software Timely Booking Button plugin <= 2.0.2 versions. **CVE ID : CVE-2023-44987**	N/A	A-GET-TIME-241123/637
Vendor: get_custom_field_values_project					
Product: get_custom_field_values					
Affected Version(s): * Up to (excluding) 4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Scott Reilly Get Custom Field Values plugin <= 4.0.1 versions. **CVE ID : CVE-2023-45604**	N/A	A-GET-GET_-241123/638
Vendor: gillesdumas					
Product: which_template_file					
Affected Version(s): * Up to (including) 4.6.0					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Gilles Dumas which template file plugin <= 4.6.0 versions. **CVE ID : CVE-2023-45753**	N/A	A-GIL-WHIC-241123/639
Vendor: Github					
Product: enterprise_server					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 3.7.18					
Incorrect Permission Assignment for Critical Resource	25-Oct-2023	2.3	Incorrect Permission Assignment for Critical Resource in GitHub Enterprise Server that allowed local operating system user accounts to read MySQL connection details including the MySQL password via configuration files. This vulnerability affected all versions of GitHub Enterprise Server and was fixed in versions 3.7.18, 3.8.11, 3.9.6, and 3.10.3. **CVE ID : CVE-2023-23767**	N/A	A-GIT-ENTE-241123/640
Affected Version(s): From (including) 3.10.0 Up to (excluding) 3.10.3					
Incorrect Permission Assignment for Critical Resource	25-Oct-2023	2.3	Incorrect Permission Assignment for Critical Resource in GitHub Enterprise Server that allowed local operating system user accounts to read MySQL connection details including the MySQL password via configuration	N/A	A-GIT-ENTE-241123/641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files. This vulnerability affected all versions of GitHub Enterprise Server and was fixed in versions 3.7.18, 3.8.11, 3.9.6, and 3.10.3. **CVE ID : CVE-2023-23767**		
Affected Version(s): From (including) 3.8.0 Up to (excluding) 3.8.11					
Incorrect Permission Assignment for Critical Resource	25-Oct-2023	2.3	Incorrect Permission Assignment for Critical Resource in GitHub Enterprise Server that allowed local operating system user accounts to read MySQL connection details including the MySQL password via configuration files. This vulnerability affected all versions of GitHub Enterprise Server and was fixed in versions 3.7.18, 3.8.11, 3.9.6, and 3.10.3. **CVE ID : CVE-2023-23767**	N/A	A-GIT-ENTE-241123/642
Affected Version(s): From (including) 3.9.0 Up to (excluding) 3.9.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	25-Oct-2023	2.3	Incorrect Permission Assignment for Critical Resource in GitHub Enterprise Server that allowed local operating system user accounts to read MySQL connection details including the MySQL password via configuration files. This vulnerability affected all versions of GitHub Enterprise Server and was fixed in versions 3.7.18, 3.8.11, 3.9.6, and 3.10.3. **CVE ID : CVE-2023-23767**	N/A	A-GIT-ENTE-241123/643
Vendor: GNU					
Product: grub2					
Affected Version(s): -					
Out-of-bounds Write	25-Oct-2023	7.8	An out-of-bounds write flaw was found in grub2's NTFS filesystem driver. This issue may allow an attacker to present a specially crafted NTFS filesystem image, leading to grub's heap metadata corruption. In	N/A	A-GNU-GRUB-241123/644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			some circumstances, the attack may also corrupt the UEFI firmware heap metadata. As a result, arbitrary code execution and secure boot protection bypass may be achieved. **CVE ID : CVE-2023-4692**		
Out-of-bounds Read	25-Oct-2023	4.6	An out-of-bounds read flaw was found on grub2's NTFS filesystem driver. This issue may allow a physically present attacker to present a specially crafted NTFS file system image to read arbitrary memory locations. A successful attack allows sensitive data cached in memory or EFI variable values to be leaked, presenting a high Confidentiality risk. **CVE ID : CVE-2023-4693**	N/A	A-GNU-GRUB-241123/645
Vendor: gofiber					
Product: fiber					
Affected Version(s): * Up to (excluding) 2.50.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Fiber is an express inspired web framework written in Go. A Cross-Site Request Forgery (CSRF) vulnerability has been identified in the application, which allows an attacker to inject arbitrary values and forge malicious requests on behalf of a user. This vulnerability can allow an attacker to inject arbitrary values without any authentication, or perform various malicious actions on behalf of an authenticated user, potentially compromising the security and integrity of the application. The vulnerability is caused by improper validation and enforcement of CSRF tokens within the application. This issue has been addressed in version 2.50.0 and users are advised to upgrade. Users should take additional security measures like	https://github.com/gofiber/fiber/security/advisories/GHSA-94w9-97p3-p368, https://github.com/gofiber/fiber/commit/8c3916dbf4ad2ed427d02c6eb63ae8b2fa8f019a	A-GOF-FIBE-241123/646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			captchas or Two-Factor Authentication (2FA) and set Session cookies with SameSite=Lax or SameSite=Secure, and the Secure and HttpOnly attributes as defense in depth measures. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45128**		
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Fiber is an express inspired web framework written in Go. A Cross-Site Request Forgery (CSRF) vulnerability has been identified in the application, which allows an attacker to obtain tokens and forge malicious requests on behalf of a user. This can lead to unauthorized actions being taken on the user's behalf, potentially compromising the security and integrity of the application. The vulnerability is caused by improper	https://github.com/gofiber/fiber/security/advisories/GHSA-mv73-f69x-444p	A-GOF-FIBE-241123/647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation and enforcement of CSRF tokens within the application. This vulnerability has been addressed in version 2.50.0 and users are advised to upgrade. Users should take additional security measures like captchas or Two-Factor Authentication (2FA) and set Session cookies with SameSite=Lax or SameSite=Secure, and the Secure and HttpOnly attributes. **CVE ID : CVE-2023-45141**		
Vendor: Golang					
Product: go					
Affected Version(s): * Up to (excluding) 1.19					
Improper Verification of Cryptographic Signature	23-Oct-2023	7.5	pkg/suci/suci.go in free5GC udm before 1.2.0, when Go before 1.19 is used, allows an Invalid Curve Attack because it may compute a shared secret via an uncompressed public key that has not been validated. An attacker can	https://github.com/free5gc/udm/pull/20	A-GOL-GO-241123/648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			send arbitrary SUCIs to the UDM, which tries to decrypt them via both its private key and the attacker's public key. **CVE ID : CVE-2023-46324**		
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 118.0.5993.117					
Use After Free	25-Oct-2023	8.8	Use after free in Profiles in Google Chrome prior to 118.0.5993.117 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-5472**	https://chromereleases.googleblog.com/2023/10/stable-channel-update-for-desktop_24.html	A-GOO-CHRO-241123/649
Vendor: gopiplus					
Product: horizontal_scrolling_announcement					
Affected Version(s): * Up to (including) 9.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Oct-2023	8.8	The Horizontal scrolling announcement plugin for WordPress is vulnerable to SQL Injection via the plugin's [horizontal-scrolling] shortcode in versions up to, and	N/A	A-GOP-HORI-241123/650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including, 9.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-4999**		
Product: image_horizontal_reel_scroll_slideshow					
Affected Version(s): * Up to (excluding) 13.3					
N/A	31-Oct-2023	6.5	The Image horizontal reel scroll slideshow plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 13.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the	https://www.wordfence.com/threat-intel/vulnerabilities/id/08fb698f-c87c-4200-85fe-3fe72745633e?source=cve, https://plugins.trac.wordpress.org/changeset/2985331/image-horizontal-	A-GOP-IMAG-241123/651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-5412**	reel-scroll-slideshow#file1	
Product: image_vertical_reel_scroll_slideshow					
Affected Version(s): * Up to (excluding) 9.1					
N/A	31-Oct-2023	6.5	The Image vertical reel scroll slideshow plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 9.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to	https://www.wordfence.com/threat-intel/vulnerabilities/id/01d31d8a-4459-488a-9cbe-92761faa58b4?source=cve, https://plugins.trac.wordpress.org/changeset/2985333/image-vertical-reel-scroll-slideshow#file1	A-GOP-IMAG-241123/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-5428**		
Affected Version(s): * Up to (including) 9.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Gopi Ramasamy Image vertical reel scroll slideshow plugin <= 9.0 versions. **CVE ID : CVE-2023-45051**	N/A	A-GOP-IMAG-241123/653
Product: information_reel					
Affected Version(s): * Up to (excluding) 10.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	31-Oct-2023	6.5	The Information Reel plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 10.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated	https://plugins.trac.wordpress.org/changeset/2985373/information-reel#file1, https://www.wordfence.com/threat-intel/vulnerabilities/id/64db63e5-ff76-494a-be4f-d820f0cc9ab0?source=cve	A-GOP-INFO-241123/654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-5429**		
Product: jquery_accordion_slideshow					
Affected Version(s): * Up to (excluding) 8.2					
N/A	31-Oct-2023	6.5	The Jquery accordion slideshow plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 8.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be	https://www.wordfence.com/threat-intel/vulnerabilities/id/0531ca34-5d7b-4071-a1aa-934f14b87728?source=cve, https://plugins.trac.wordpress.org/changeset/2985511/jquery-accordion-slideshow#file0	A-GOP-JQUE-241123/655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used to extract sensitive information from the database. **CVE ID : CVE-2023-5464**		
Product: jquery_news_ticker					
Affected Version(s): * Up to (excluding) 3.1					
N/A	31-Oct-2023	6.5	The Jquery news ticker plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 3.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-5430**	https://plugins.trac.wordpress.org/changeset/2985559/jquery-news-ticker#file1	A-GOP-JQUE-241123/656
Product: left_right_image_slideshow_gallery					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 12.1					
N/A	31-Oct-2023	6.5	The Left right image slideshow gallery plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 12.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-5431**	https://www.wordfence.com/threat-intel/vulnerabilities/id/69902627-ce79-4a43-8949-43db6a9cc0dd?source=cve, https://plugins.trac.wordpress.org/changeset/2985417/left-right-image-slideshow-gallery#file0	A-GOP-LEFT-241123/657
Product: message_ticker					
Affected Version(s): * Up to (excluding) 9.3					
N/A	31-Oct-2023	6.5	The Message ticker plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode	https://www.wordfence.com/threat-intel/vulnerabilities/id/d0b1fa88-2fc6-41af-	A-GOP-MESS-241123/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in versions up to, and including, 9.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-5433**	bd39-12af92dc6533?source=cve, https://plugins.trac.wordpress.org/changeset/2985499/message-ticker#file1	
Product: scroll_post_excerpt					
Affected Version(s): * Up to (including) 8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Gopi Ramasamy Scroll post excerpt plugin <= 8.0 versions. **CVE ID : CVE-2023-45764**	N/A	A-GOP-SCRO-241123/659
Product: superb_slideshow_gallery					
Affected Version(s): * Up to (excluding) 13.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	31-Oct-2023	6.5	The Superb slideshow gallery plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 13.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-5434**	https://plugins.trac.wordpress.org/changeset/2985501/superb-slideshow-gallery#file2, https://www.wordfence.com/threat-intel/vulnerabilities/id/3a12945d-a67c-4a19-a4e7-f65f5f2a21bb?source=cve	A-GOP-SUPE-241123/660
Product: tiny_carosel_horizontal_slider					
Affected Version(s): * Up to (including) 8.1					
Improper Neutralization of Input During Web Page Generation	16-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Gopi Ramasamy Tiny Carousel Horizontal Slider	N/A	A-GOP-TINY-241123/661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			plugin <= 8.1 versions. **CVE ID : CVE-2023-44229**		
Product: up_down_image_slideshow_gallery					
Affected Version(s): * Up to (excluding) 12.1					
N/A	31-Oct-2023	6.5	The Up down image slideshow gallery plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 12.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-5435**	https://www.wordfence.com/threat-intel/vulnerabilities/id/0b72cf6f-4924-4fa5-8e1a-4054dfe73be0?source=cve, https://plugins.trac.wordpress.org/changeset/2985497/up-down-image-slideshow-gallery#file1	A-GOP-UP_D-241123/662
Product: vertical_marquee_plugin					
Affected Version(s): * Up to (excluding) 7.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	31-Oct-2023	6.5	The Vertical marquee plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 7.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-5436**	https://www.wordfence.com/threat-intel/vulnerabilities/id/cd90d9c0-0cab-4fd3-b016-106032f300f7?source=cve, https://plugins.trac.wordpress.org/changeset/2985561/vertical-marquee-plugin#file2	A-GOP-VERT-241123/663
Product: wp_fade_in_text_news					
Affected Version(s): * Up to (excluding) 12.1					
N/A	31-Oct-2023	6.5	The WP fade in text news plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 12.0 due to insufficient	https://www.wordfence.com/threat-intel/vulnerabilities/id/b4accf10-710e-4cba-8d61-04e422324f9d?source=cve,	A-GOP-WP_F-241123/664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-5437**	https://plugins.trac.wordpress.org/changeset/2985398/wp-fade-in-text-news#file2	
Product: wp_image_slideshow					
Affected Version(s): * Up to (excluding) 12.1					
N/A	31-Oct-2023	6.5	The wp image slideshow plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 12.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated	https://plugins.trac.wordpress.org/changeset/2985394/wp-image-slideshow#file2, https://www.wordfence.com/threat-intel/vulnerabilities/id/7e24383b-5b0f-4114-908b-4c2778632f73?source=cve	A-GOP-WP_I-241123/665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-5438**		
Product: wp_photo_text_slider_50					
Affected Version(s): * Up to (excluding) 8.1					
N/A	31-Oct-2023	6.5	The Wp photo text slider 50 plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 8.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract	https://plugins.trac.wordpress.org/changeset/2985502/wp-photo-text-slider-50#file1, https://www.wordfence.com/threat-intel/vulnerabilities/id/515502b5-c344-4855-aff1-57833233c5d2?source=cve	A-GOP-WP_P-241123/666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive information from the database. **CVE ID : CVE-2023-5439**		
Vendor: gougucms					
Product: gougucms					
Affected Version(s): 4.08.18					
N/A	27-Oct-2023	7.5	gougucms v4.08.18 was discovered to contain a password reset poisoning vulnerability which allows attackers to arbitrarily reset users' passwords via a crafted packet. **CVE ID : CVE-2023-46393**	N/A	A-GOU-GOUG-241123/667
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	5.4	A stored cross-site scripting (XSS) vulnerability in /home/user/edit_submit of gougucms v4.08.18 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the headimgurl parameter. **CVE ID : CVE-2023-46394**	N/A	A-GOU-GOUG-241123/668
Vendor: gowebsolutions					
Product: wp_customer_reviews					
Affected Version(s): * Up to (excluding) 3.6.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	4.8	The WP Customer Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 3.6.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-4648**	https://plugins.trac.wordpress.org/changeset/2965658/wp-customer-reviews/trunk?contextall=1&old=2882143&old_path=%2Fwp-customer-reviews%2Ftrunk	A-GOW-WP_C-241123/669
Vendor: gpac					
Product: gpac					
Affected Version(s): * Up to (excluding) 2.3.0					
N/A	16-Oct-2023	5.5	Denial of Service in GitHub repository gpac/gpac prior to 2.3.0-DEV. **CVE ID : CVE-2023-5595**	https://github.com/gpac/gpac/commit/7a6f636db3360bb16d18078d51e8c596f31302a1	A-GPA-GPAC-241123/670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: grafana					
Product: google_sheets					
Affected Version(s): From (including) 0.9.0 Up to (including) 1.2.2					
Generation of Error Message Containing Sensitive Information	16-Oct-2023	7.5	Grafana is an open-source platform for monitoring and observability. The Google Sheets data source plugin for Grafana, versions 0.9.0 to 1.2.2 are vulnerable to an information disclosure vulnerability. The plugin did not properly sanitize error messages, making it potentially expose the Google Sheet API-key that is configured for the data source. This vulnerability was fixed in version 1.2.2. **CVE ID : CVE-2023-4457**	https://grafana.com/security/security-advisories/cve-2023-4457/	A-GRA-GOOG-241123/671
Product: grafana					
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.0.7					
N/A	16-Oct-2023	7.2	Grafana is an open-source platform for monitoring and observability. The vulnerability impacts Grafana instances with several organizations, and	https://grafana.com/security/security-advisories/cve-2023-4822	A-GRA-GRAF-241123/672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a user with Organization Admin permissions in one organization to change the permissions associated with Organization Viewer, Organization Editor and Organization Admin roles in all organizations. It also allows an Organization Admin to assign or revoke any permissions that they have to any user globally. This means that any Organization Admin can elevate their own permissions in any organization that they are already a member of, or elevate or restrict the permissions of any other user. The vulnerability does not allow a user to become a member of an organization that they are not already a member of, or to add any other users to an organization that		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the current user is not a member of. **CVE ID : CVE-2023-4822**		
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.0.9					
N/A	17-Oct-2023	7.2	Grafana is an open-source platform for monitoring and observability. In Grafana Enterprise, Request security is a deny list that allows admins to configure Grafana in a way so that the instance doesn't call specific hosts. However, the restriction can be bypassed used punycode encoding of the characters in the request address. **CVE ID : CVE-2023-4399**	https://grafana.com/security/security-advisories/cve-2023-4399/	A-GRA-GRAF-241123/673
Affected Version(s): From (including) 10.1.0 Up to (excluding) 10.1.3					
N/A	16-Oct-2023	7.2	Grafana is an open-source platform for monitoring and observability. The vulnerability impacts Grafana instances with several organizations, and allows a user with Organization Admin permissions in one organization	https://grafana.com/security/security-advisories/cve-2023-4822	A-GRA-GRAF-241123/674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to change the permissions associated with Organization Viewer, Organization Editor and Organization Admin roles in all organizations. It also allows an Organization Admin to assign or revoke any permissions that they have to any user globally. This means that any Organization Admin can elevate their own permissions in any organization that they are already a member of, or elevate or restrict the permissions of any other user. The vulnerability does not allow a user to become a member of an organization that they are not already a member of, or to add any other users to an organization that the current user is not a member of. **CVE ID : CVE-2023-4822**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 10.1.0 Up to (excluding) 10.1.5					
N/A	17-Oct-2023	7.2	Grafana is an open-source platform for monitoring and observability. In Grafana Enterprise, Request security is a deny list that allows admins to configure Grafana in a way so that the instance doesn't call specific hosts. However, the restriction can be bypassed used punycode encoding of the characters in the request address. **CVE ID : CVE-2023-4399**	https://grafana.com/security/security-advisories/cve-2023-4399/	A-GRA-GRAF-241123/675
Affected Version(s): From (including) 8.0.0 Up to (excluding) 9.4.16					
N/A	16-Oct-2023	7.2	Grafana is an open-source platform for monitoring and observability. The vulnerability impacts Grafana instances with several organizations, and allows a user with Organization Admin permissions in one organization to change the permissions associated with Organization Viewer,	https://grafana.com/security/security-advisories/cve-2023-4822	A-GRA-GRAF-241123/676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Organization Editor and Organization Admin roles in all organizations. It also allows an Organization Admin to assign or revoke any permissions that they have to any user globally. This means that any Organization Admin can elevate their own permissions in any organization that they are already a member of, or elevate or restrict the permissions of any other user. The vulnerability does not allow a user to become a member of an organization that they are not already a member of, or to add any other users to an organization that the current user is not a member of. **CVE ID : CVE-2023-4822**		
Affected Version(s): From (including) 9.4.0 Up to (excluding) 9.4.17					
N/A	17-Oct-2023	7.2	Grafana is an open-source platform for monitoring and observability.	https://grafana.com/security/security-	A-GRA-GRAF-241123/677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			In Grafana Enterprise, Request security is a deny list that allows admins to configure Grafana in a way so that the instance doesn't call specific hosts. However, the restriction can be bypassed used punycode encoding of the characters in the request address. **CVE ID : CVE-2023-4399**	advisories/cve-2023-4399/	
Affected Version(s): From (including) 9.5.0 Up to (excluding) 9.5.11					
N/A	16-Oct-2023	7.2	Grafana is an open-source platform for monitoring and observability. The vulnerability impacts Grafana instances with several organizations, and allows a user with Organization Admin permissions in one organization to change the permissions associated with Organization Viewer, Organization Editor and Organization Admin roles in all organizations.	https://grafana.com/security/security-advisories/cve-2023-4822	A-GRA-GRAF-241123/678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			It also allows an Organization Admin to assign or revoke any permissions that they have to any user globally. This means that any Organization Admin can elevate their own permissions in any organization that they are already a member of, or elevate or restrict the permissions of any other user. The vulnerability does not allow a user to become a member of an organization that they are not already a member of, or to add any other users to an organization that the current user is not a member of. **CVE ID : CVE-2023-4822**		
Affected Version(s): From (including) 9.5.0 Up to (excluding) 9.5.13					
N/A	17-Oct-2023	7.2	Grafana is an open-source platform for monitoring and observability. In Grafana Enterprise, Request security is a deny list that allows admins to	https://grafana.com/security/security-advisories/cve-2023-4399/	A-GRA-GRAF-241123/679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configure Grafana in a way so that the instance doesn't call specific hosts. However, the restriction can be bypassed used punycode encoding of the characters in the request address. **CVE ID : CVE-2023-4399**		
Product: worldmap_panel					
Affected Version(s): * Up to (excluding) 1.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	6.1	Grafana is an open-source platform for monitoring and observability. The WorldMap panel plugin, versions before 1.0.4 contains a DOM XSS vulnerability. **CVE ID : CVE-2023-3010**	https://grafana.com/security/security-advisories/cve-2023-3010/	A-GRA-WORL-241123/680
Vendor: groundhogg					
Product: groundhogg					
Affected Version(s): * Up to (excluding) 2.7.11.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Groundhogg Inc. Groundhogg plugin <= 2.7.11.10 versions. **CVE ID : CVE-2023-40681**	N/A	A-GRO-GROU-241123/681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: gumroad					
Product: gumroad					
Affected Version(s): * Up to (including) 3.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Gumroad plugin <= 3.1.0 versions. **CVE ID : CVE-2023-45059**	N/A	A-GUM-GUMR-241123/682
Vendor: gvectors					
Product: wpdiscuz					
Affected Version(s): * Up to (including) 7.6.3					
Missing Authorization	20-Oct-2023	5.3	The wpDiscuz plugin for WordPress is vulnerable to unauthorized modification of data due to a missing authorization check on the voteOnComment function in versions up to, and including, 7.6.3. This makes it possible for unauthenticated attackers to increase or decrease the rating of a comment. **CVE ID : CVE-2023-3869**	N/A	A-GVE-WPDI-241123/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	20-Oct-2023	5.3	The wpDiscuz plugin for WordPress is vulnerable to unauthorized modification of data due to a missing authorization check on the userRate function in versions up to, and including, 7.6.3. This makes it possible for unauthenticated attackers to increase or decrease the rating of a post. **CVE ID : CVE-2023-3998**	N/A	A-GVE-WPDI-241123/684
Vendor: halgatewood					
Product: reusable_text_blocks					
Affected Version(s): * Up to (including) 1.5.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	The Reusable Text Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'text-blocks' shortcode in versions up to, and including, 1.5.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated	N/A	A-HAL-REUS-241123/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers with author-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5745**		
Vendor: hallowelt					
Product: bluespice					
Affected Version(s): From (including) 3.0 Up to (excluding) 3.2.10.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Oct-2023	5.4	Cross-site Scripting (XSS) vulnerability in BlueSpiceAvatars extension of BlueSpice allows logged in user to inject arbitrary HTML into the profile image dialog on Special:Preferences. This only applies to the genuine user context. **CVE ID : CVE-2023-42431**	N/A	A-HAL-BLUE-241123/686
Affected Version(s): From (including) 4.0 Up to (excluding) 4.3.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Oct-2023	5.4	Cross-site Scripting (XSS) vulnerability in BlueSpiceAvatars extension of BlueSpice allows logged in user to inject arbitrary HTML into the	N/A	A-HAL-BLUE-241123/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			profile image dialog on Special:Preferences. This only applies to the genuine user context. **CVE ID : CVE-2023-42431**		
Vendor: happybox					
Product: newsletter_\&_bulk_email_sender					
Affected Version(s): * Up to (including) 2.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in HappyBox Newsletter & Bulk Email Sender – Email Newsletter Plugin for WordPress plugin <= 2.0.1 versions. **CVE ID : CVE-2023-45829**	N/A	A-HAP-NEWS-241123/688
Vendor: Haxx					
Product: libcurl					
Affected Version(s): From (including) 7.69.0 Up to (excluding) 8.4.0					
Out-of-bounds Write	18-Oct-2023	9.8	This flaw makes curl overflow a heap based buffer in the SOCKS5 proxy handshake. When curl is asked to pass along the host name to the	https://curl.se/docs/CVE-2023-38545.html	A-HAX-LIBC-241123/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SOCKS5 proxy to allow that to resolve the address instead of it getting done by curl itself, the maximum length that host name can be is 255 bytes. If the host name is detected to be longer, curl switches to local name resolving and instead passes on the resolved address only. Due to this bug, the local variable that means "let the host resolve the name" could get the wrong value during a slow SOCKS5 handshake, and contrary to the intention, copy the too long host name to the target buffer instead of copying just the resolved address there. The target buffer being a heap based		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer, and the host name coming from the URL that curl has been told to operate with. **CVE ID : CVE-2023-38545**		
Affected Version(s): From (including) 7.9.1 Up to (excluding) 8.4.0					
N/A	18-Oct-2023	3.7	This flaw allows an attacker to insert cookies at will into a running program using libcurl, if the specific series of conditions are met. libcurl performs transfers. In its API, an application creates "easy handles" that are the individual handles for single transfers. libcurl provides a function call that duplicates en easy handle called [curl_easy_duphandle](https://curl.se/libcurl/c/curl_easy_duphandle.html). If a transfer has cookies enabled when the handle is duplicated, the cookie-enable state is also cloned - but	https://curl.se/docs/CVE-2023-38546.html	A-HAX-LIBC-241123/690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without cloning the actual cookies. If the source handle did not read any cookies from a specific file on disk, the cloned version of the handle would instead store the file name as `none` (using the four ASCII letters, no quotes). Subsequent use of the cloned handle that does not explicitly set a source to load cookies from would then inadvertently load cookies from a file named `none` - if such a file exists and is readable in the current directory of the program using libcurl. And if using the correct file format of course. **CVE ID : CVE-2023-38546**		
Vendor: hcltech					
Product: appscan_presence					
Affected Version(s): * Up to (including) 2.1.37					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unquoted Search Path or Element	17-Oct-2023	7.8	An unquoted service path vulnerability in HCL AppScan Presence, deployed as a Windows service in HCL AppScan on Cloud (ASoC), may allow a local attacker to gain elevated privileges. **CVE ID : CVE-2023-37537**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0108018	A-HCL-APPS-241123/691
Product: commerce					
Affected Version(s): From (including) 9.1.8 Up to (including) 9.1.13.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Oct-2023	4.3	HCL Commerce Remote Store server could allow a remote attacker, using a specially-crafted URL, to read arbitrary files on the system. **CVE ID : CVE-2023-37532**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0108094	A-HCL-COMM-241123/692
Product: hcl_compass					
Affected Version(s): 2.1.0					
Weak Password Requirements	19-Oct-2023	9.8	HCL Compass is vulnerable to insecure password requirements. An attacker could easily guess the password and gain access to user accounts. **CVE ID : CVE-2023-37503**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0107512	A-HCL-HCL_-241123/693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	18-Oct-2023	8.8	HCL Compass is vulnerable to lack of file upload security. An attacker could upload files containing active code that can be executed by the server or by a user's web browser. **CVE ID : CVE-2023-37502**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0107510	A-HCL-HCL_-241123/694
Insufficient Session Expiration	19-Oct-2023	6.5	HCL Compass is vulnerable to failure to invalidate sessions. The application does not invalidate authenticated sessions when the log out functionality is called. If the session identifier can be discovered, it could be replayed to the application and used to impersonate the user. **CVE ID : CVE-2023-37504**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0107511	A-HCL-HCL_-241123/695
Affected Version(s): From (including) 2.0.0 Up to (including) 2.0.3					
Weak Password Requirements	19-Oct-2023	9.8	HCL Compass is vulnerable to insecure password requirements. An attacker could easily guess the	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0107512	A-HCL-HCL_-241123/696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password and gain access to user accounts. **CVE ID : CVE-2023-37503**		
Unrestricted Upload of File with Dangerous Type	18-Oct-2023	8.8	HCL Compass is vulnerable to lack of file upload security. An attacker could upload files containing active code that can be executed by the server or by a user's web browser. **CVE ID : CVE-2023-37502**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0107510	A-HCL-HCL_-241123/697
Insufficient Session Expiration	19-Oct-2023	6.5	HCL Compass is vulnerable to failure to invalidate sessions. The application does not invalidate authenticated sessions when the log out functionality is called. If the session identifier can be discovered, it could be replayed to the application and used to impersonate the user. **CVE ID : CVE-2023-37504**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0107511	A-HCL-HCL_-241123/698
Affected Version(s): From (including) 2.2.0 Up to (excluding) 2.2.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weak Password Requirements	19-Oct-2023	9.8	HCL Compass is vulnerable to insecure password requirements. An attacker could easily guess the password and gain access to user accounts. **CVE ID : CVE-2023-37503**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0107512	A-HCL-HCL_-241123/699
Unrestricted Upload of File with Dangerous Type	18-Oct-2023	8.8	HCL Compass is vulnerable to lack of file upload security. An attacker could upload files containing active code that can be executed by the server or by a user's web browser. **CVE ID : CVE-2023-37502**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0107510	A-HCL-HCL_-241123/700
Insufficient Session Expiration	19-Oct-2023	6.5	HCL Compass is vulnerable to failure to invalidate sessions. The application does not invalidate authenticated sessions when the log out functionality is called. If the session identifier can be discovered, it could be replayed to the application and used to	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0107511	A-HCL-HCL_-241123/701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impersonate the user. **CVE ID : CVE-2023-37504**		
Vendor: hdclic					
Product: prestablog					
Affected Version(s): * Up to (excluding) 4.4.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	31-Oct-2023	9.8	In the module "PrestaBlog" (prestablog) version 4.4.7 and before from HDclic for PrestaShop, a guest can perform SQL injection. The script ajax slider_positions.php has a sensitive SQL call that can be executed with a trivial http call and exploited to forge a SQL injection. **CVE ID : CVE-2023-45378**	https://security.friendsofpresta.org/modules/2023/10/26/prestablog.html	A-HDC-PRES-241123/702
Vendor: helmholz					
Product: myrex24					
Affected Version(s): * Up to (including) 2.14.2					
Improper Privilege Management	16-Oct-2023	4.3	In Red Lion Europe mbCONNECT24 and mymbCONNECT24 and Helmholz myREX24 and myREX24.virtual up to and including 2.14.2 an improperly implemented access validation allows an	N/A	A-HEL-MYRE-241123/703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, low privileged attacker to gain read access to limited, non-critical device information in his account he should not have access to. **CVE ID : CVE-2023-4834**		
Product: myrex24.virtual					
Affected Version(s): * Up to (including) 2.14.2					
Improper Privilege Management	16-Oct-2023	4.3	In Red Lion Europe mbCONNECT24 and mymbCONNECT24 and Helmholz myREX24 and myREX24.virtual up to and including 2.14.2 an improperly implemented access validation allows an authenticated, low privileged attacker to gain read access to limited, non-critical device information in his account he should not have access to. **CVE ID : CVE-2023-4834**	N/A	A-HEL-MYRE-241123/704
Vendor: henryholtgeerts					
Product: pdf_block					
Affected Version(s): * Up to (including) 1.1.0					
Improper Neutralization of	25-Oct-2023	5.4	Auth. (contributor+) Stored Cross-Site	N/A	A-HEN-PDF_-241123/705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Scripting (XSS) vulnerability in Henryholtgeerts PDF Block plugin <= 1.1.0 versions. **CVE ID : CVE-2023-45646**		
Vendor: hestiacp					
Product: control_panel					
Affected Version(s): * Up to (excluding) 1.8.9					
Privilege Chaining	29-Oct-2023	7.8	Privilege Chaining in GitHub repository hestiacp/hestiacp prior to 1.8.9. **CVE ID : CVE-2023-5839**	https://huntr.com/bounties/21125f12-64a0-42a3-b218-26b9945a5bc0, https://github.com/hestiacp/hestiacp/commit/acb766e1db53de70534524b3fbc2270689112630	A-HES-CONT-241123/706
Vendor: hipresta					
Product: carousels_pack					
Affected Version(s): * Up to (excluding) 1.5.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Oct-2023	9.8	In the module "Carousels Pack - Instagram, Products, Brands, Supplier" (hicarouselspack) for PrestaShop up to version 1.5.0 from HiPresta for PrestaShop, a guest can perform SQL injection via HiCpProductGetter::getViewedProduct().`	N/A	A-HIP-CARO-241123/707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45376		
Vendor: hitsteps					
Product: web_analytics					
Affected Version(s): * Up to (including) 5.86					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Hitsteps Web Analytics plugin <= 5.86 versions. **CVE ID : CVE-2023-45057**	N/A	A-HIT-WEB_-241123/708
Vendor: home-assistant					
Product: home-assistant					
Affected Version(s): * Up to (excluding) 2023.8.0					
Insufficient Verification of Data Authenticity	19-Oct-2023	9	Home assistant is an open source home automation. Whilst auditing the frontend code to identify hidden parameters, Cure53 detected `auth_callback=1`, which is leveraged by the WebSocket authentication logic in tandem with the `state` parameter. The state parameter contains the `hassUrl`, which is subsequently utilized to establish a WebSocket connection. This behavior permits an attacker to	https://github.com/home-assistant/core/security/advisories/GHSA-cr83-q7r2-7f5q	A-HOM-HOME-241123/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			create a malicious Home Assistant link with a modified state parameter that forces the frontend to connect to an alternative WebSocket backend. Henceforth, the attacker can spoof any WebSocket responses and trigger cross site scripting (XSS). Since the XSS is executed on the actual Home Assistant frontend domain, it can connect to the real Home Assistant backend, which essentially represents a comprehensive takeover scenario. Permitting the site to be iframed by other origins, as discussed in GHSA-935v-rmg9-44mw, renders this exploit substantially covert since a malicious website can obfuscate the compromise strategy in the background. However, even without this, the attacker can still		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			send the `auth_callback` link directly to the victim user. To mitigate this issue, Cure53 advises modifying the WebSocket code's authentication flow. An optimal implementation in this regard would not trust the `hassUrl` passed in by a GET parameter. Cure53 must stipulate the significant time required of the Cure53 consultants to identify an XSS vector, despite holding full control over the WebSocket responses. In many areas, data from the WebSocket was properly sanitized, which hinders post-exploitation. The audit team eventually detected the `js_url` for custom panels, though generally, the frontend exhibited reasonable security hardening. This issue has been addressed in Home Assistant Core version 2023.8.0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and in the npm package home-assistant-js-websocket in version 8.2.0. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-41896**		
Affected Version(s): * Up to (excluding) 2023.9.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2023	9.6	Home assistant is an open source home automation. The Home Assistant login page allows users to use their local Home Assistant credentials and log in to another website that specifies the `redirect_uri` and `client_id` parameters. Although the `redirect_uri` validation typically ensures that it matches the `client_id` and the scheme represents either `http` or `https`, Home Assistant will fetch the `client_id` and check for `<link rel="redirect_uri" href="...">` HTML tags on the page.	https://github.com/home-assistant/core/security/advisories/GHSA-jvxq-x42r-f7mv	A-HOM-HOME-241123/710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These URLs are not subjected to the same scheme validation and thus allow for arbitrary JavaScript execution on the Home Assistant administration page via usage of `javascript:` scheme URIs. This Cross-site Scripting (XSS) vulnerability can be executed on the Home Assistant frontend domain, which may be used for a full takeover of the Home Assistant account and installation. This issue has been addressed in version 2023.9.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-41895**		
Improper Restriction of Rendered UI Layers or Frames	19-Oct-2023	9.6	Home assistant is an open source home automation. Home Assistant server does not set any HTTP security headers, including the X-Frame-Options header, which specifies	https://www.home-assistant.io/blog/2023/10/19/security-audits-of-home-assistant/, https://github.com/home-assistant/core/	A-HOM-HOME-241123/711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			whether the web page is allowed to be framed. The omission of this and correlating headers facilitates covert clickjacking attacks and alternative exploit opportunities, such as the vector described in this security advisory. This fault incurs major risk, considering the ability to trick users into installing an external and malicious add-on with minimal user interaction, which would enable Remote Code Execution (RCE) within the Home Assistant application. This issue has been addressed in version 2023.9.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-41897**	security/advisories/GHSA-935v-rmg9-44mw	
Server-Side Request	19-Oct-2023	7.2	Home assistant is an open source home automation.	https://github.com/home-assistant/core/	A-HOM-HOME-241123/712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			In affected versions the `hassio.addon_stdin` is vulnerable to a partial Server-Side Request Forgery where an attacker capable of calling this service (e.g.: through GHSA-h2jp-7grc-9xpp) may be able to invoke any Supervisor REST API endpoints with a POST request. An attacker able to exploit will be able to control the data dictionary, including its addon and input key/values. This issue has been addressed in version 2023.9.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability. This issue is also tracked as GitHub Security Lab (GHSL) Vulnerability Report: `GHSL-2023-162`. **CVE ID : CVE-2023-41899**	security/advisories/GHSA-h2jp-7grc-9xpp, https://github.com/home-assistant/core/security/advisories/GHSA-4r74-h49q-rr3h	
N/A	20-Oct-2023	5.4	Home assistant is an open source	https://www.home-	A-HOM-HOME-241123/713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			home automation. The audit team's analyses confirmed that the `redirect_uri` and `client_id` are alterable when logging in. Consequently, the code parameter utilized to fetch the `access_token` post-authentication will be sent to the URL specified in the aforementioned parameters. Since an arbitrary URL is permitted and `homeassistant.local` represents the preferred, default domain likely used and trusted by many users, an attacker could leverage this weakness to manipulate a user and retrieve account access. Notably, this attack strategy is plausible if the victim has exposed their Home Assistant to the Internet, since after acquiring the victim's `access_token` the adversary would need to utilize it	assistant.io/blog/2023/10/19/security-audits-of-home-assistant/, https://github.com/home-assistant/core/security/advisories/GHSA-qhhj-7hrc-gqj5	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			directly towards the instance to achieve any pertinent malicious actions. To achieve this compromise attempt, the attacker must send a link with a `redirect_uri` that they control to the victim's own Home Assistant instance. In the eventuality the victim authenticates via said link, the attacker would obtain code sent to the specified URL in `redirect_uri`, which can then be leveraged to fetch an `access_token`. Pertinently, an attacker could increase the efficacy of this strategy by registering a near identical domain to `homeassistant.local`, which at first glance may appear legitimate and thereby obfuscate any malicious intentions. This issue has been addressed in version 2023.9.0 and all users are advised to upgrade. There are no		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known workarounds for this vulnerability. **CVE ID : CVE-2023-41893**		
N/A	20-Oct-2023	5.3	Home assistant is an open source home automation. The assessment verified that webhooks available in the webhook component are triggerable via the `*.ui.nabu.casa` URL without authentication, even when the webhook is marked as Only accessible from the local network. This issue is facilitated by the SniTun proxy, which sets the source address to 127.0.0.1 on all requests sent to the public URL and forwarded to the local Home Assistant. This issue has been addressed in version 2023.9.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	https://github.com/home-assistant/core/security/advisories/GHSA-wx3j-3v2j-rf45, https://www.home-assistant.io/blog/2023/10/19/security-audits-of-home-assistant/	A-HOM-HOME-241123/714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-41894		
Product: home-assistant-js-websocket					
Affected Version(s): * Up to (excluding) 8.2.0					
Insufficient Verification of Data Authenticity	19-Oct-2023	9	Home assistant is an open source home automation. Whilst auditing the frontend code to identify hidden parameters, Cure53 detected `auth_callback=1`, which is leveraged by the WebSocket authentication logic in tandem with the `state` parameter. The state parameter contains the `hassUrl`, which is subsequently utilized to establish a WebSocket connection. This behavior permits an attacker to create a malicious Home Assistant link with a modified state parameter that forces the frontend to connect to an alternative WebSocket backend. Henceforth, the attacker can spoof any WebSocket responses and trigger cross site	https://github.com/home-assistant/core/security/advisories/GHSA-cr83-q7r2-7f5q	A-HOM-HOME-241123/715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting (XSS). Since the XSS is executed on the actual Home Assistant frontend domain, it can connect to the real Home Assistant backend, which essentially represents a comprehensive takeover scenario. Permitting the site to be iframed by other origins, as discussed in GHSA-935v-rmg9-44mw, renders this exploit substantially covert since a malicious website can obfuscate the compromise strategy in the background. However, even without this, the attacker can still send the `auth_callback` link directly to the victim user. To mitigate this issue, Cure53 advises modifying the WebSocket code's authentication flow. An optimal implementation in this regard would not trust the `hassUrl` passed in by a GET		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter. Cure53 must stipulate the significant time required of the Cure53 consultants to identify an XSS vector, despite holding full control over the WebSocket responses. In many areas, data from the WebSocket was properly sanitized, which hinders post-exploitation. The audit team eventually detected the `js_url` for custom panels, though generally, the frontend exhibited reasonable security hardening. This issue has been addressed in Home Assistant Core version 2023.8.0 and in the npm package home-assistant-js-websocket in version 8.2.0. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-41896**		
Product: home_assistant_companion					
Affected Version(s): * Up to (excluding) 2023.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	19-Oct-2023	8.8	The Home Assistant Companion for iOS and macOS app up to version 2023.4 are vulnerable to Client-Side Request Forgery. Attackers may send malicious links/QRs to victims that, when visited, will make the victim to call arbitrary services in their Home Assistant installation. Combined with this security advisory, may result in full compromise and remote code execution (RCE). Version 2023.7 addresses this issue and all users are advised to upgrade. There are no known workarounds for this vulnerability. This issue is also tracked as GitHub Security Lab (GHSL) Vulnerability Report: GHSL-2023-161. **CVE ID : CVE-2023-44385**	https://github.com/home-assistant/core/security/advisories/GHSA-h2jp-7grc-9xpp	A-HOM-HOME-241123/716
Affected Version(s): * Up to (excluding) 2023.9.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	19-Oct-2023	7.8	Home assistant is an open source home automation. The Home Assistant Companion for Android app up to version 2023.8.2 is vulnerable to arbitrary URL loading in a WebView. This enables all sorts of attacks, including arbitrary JavaScript execution, limited native code execution, and credential theft. This issue has been patched in version 2023.9.2 and all users are advised to upgrade. There are no known workarounds for this vulnerability. This issue is also tracked as GitHub Security Lab (GHSL) Vulnerability Report: `GHSL-2023-142`. **CVE ID : CVE-2023-41898**	https://github.com/home-assistant/core/security/advisories/GHSA-jvpm-q3hq-86rg	A-HOM-HOME-241123/717
Vendor: hoosoft					
Product: magee_shortcodes					
Affected Version(s): * Up to (including) 2.1.1					
N/A	16-Oct-2023	5.4	The Magee Shortcodes	N/A	A-HOO-MAGE-241123/718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WordPress plugin through 2.1.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-4783**		
Vendor: HP					
Product: print_and_scan_doctor					
Affected Version(s): 5.7.2.014					
N/A	25-Oct-2023	7.8	HP Print and Scan Doctor for Windows may potentially be vulnerable to escalation of privilege. HP is releasing software updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-5671**	https://support.hp.com/us-en/document/ish_9502679-9502704-16	A-HP-PRIN-241123/719
Vendor: hpe					
Product: oneview					
Affected Version(s): * Up to (excluding) 8.60.00					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Oct-2023	9.8	A remote code execution issue exists in HPE OneView. **CVE ID : CVE-2023-30912**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04548en_us	A-HPE-ONEV-241123/720
Vendor: hu60					
Product: hu60wap6					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Oct-2023	6.1	A vulnerability classified as problematic was found in hu60t hu60wap6. Affected by this vulnerability is the function markdown of the file src/class/ubbparser.php. The manipulation leads to cross site scripting. The attack can be launched remotely. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The patch is named a1cd9f12d7687243bfcb7ce295665acb83b9174e. It is recommended to	https://github.com/hu60t/hu60wap6/commit/a1cd9f12d7687243bfcb7ce295665acb83b9174e	A-HU6-HU60-241123/721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-243775. **CVE ID : CVE-2023-5835**		
Vendor: hynotech					
Product: dropbox_folder_share					
Affected Version(s): * Up to (including) 1.9.7					
Inclusion of Functionality from Untrusted Control Sphere	20-Oct-2023	9.8	The Dropbox Folder Share for WordPress is vulnerable to Local File Inclusion in versions up to, and including, 1.9.7 via the editor-view.php file. This allows unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included. **CVE ID : CVE-2023-4488**	https://www.wordfence.com/threat-intel/vulnerabilities/id/647a2f27-092a-4db1-932d-87ae8c2efcca?source=cve, https://plugins.trac.wordpress.org/browser/dropbox-folder-share/trunk/HynoTech/UsosGenerales/js/editor-view.php?rev=2904670	A-HYN-DROP-241123/722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: I-doit					
Product: i-doit					
Affected Version(s): * Up to (including) 25					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-2023	5.4	I-doit pro 25 and below is vulnerable to Cross Site Scripting (XSS) via index.php. **CVE ID : CVE-2023-46003**	N/A	A-I-D-I-DO-241123/723
Vendor: i13websolution					
Product: easy_testimonial_slider_and_form					
Affected Version(s): * Up to (including) 1.0.18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution Easy Testimonial Slider and Form plugin <= 1.0.18 versions. **CVE ID : CVE-2023-45754**	N/A	A-I13-EASY-241123/724
Product: thumbnail_carousel_slider					
Affected Version(s): 1.0					
N/A	27-Oct-2023	6.5	The Thumbnail carousel slider plugin for WordPress is vulnerable to Cross-Site Request Forgery in version 1.0. This is due to missing nonce validation on the deleteselected function. This	N/A	A-I13-THUM-241123/725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			makes it possible for unauthenticated attackers to delete sliders in bulk via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-5821**		
Product: thumbnail_slider_with_lightbox					
Affected Version(s): 1.0					
Cross-Site Request Forgery (CSRF)	27-Oct-2023	8.8	The Thumbnail Slider With Lightbox plugin for WordPress is vulnerable to Cross-Site Request Forgery in version 1.0. This is due to missing or incorrect nonce validation on the addedit functionality. This makes it possible for unauthenticated attackers to upload arbitrary files via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=1263536%40wp-responsive-slider-with-lightbox&new=1263536%40wp-responsive-slider-with-lightbox&sfp_email=&sfph_mail=	A-I13-THUM-241123/726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5820		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	4.8	The Thumbnail Slider With Lightbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Image Title field in versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-5621**	N/A	A-I13-THUM-241123/727
Vendor: IBM					
Product: cics_tx					
Affected Version(s): 10.1					
Uncontrolled Resource	25-Oct-2023	4.9	IBM TXSeries for Multiplatforms, 8.1, 8.2, and 9.1, CICS TX Standard CICS	https://www.ibm.com/support/pages/node/7056429,	A-IBM-CICS-241123/728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			TX Advanced 10.1 and 11.1 could allow a privileged user to cause a denial of service due to uncontrolled resource consumption. IBM X-Force ID: 266016. **CVE ID : CVE-2023-42031**	https://exchange.xforce.ibmcloud.com/vulnerabilities/266061, https://www.ibm.com/support/pages/node/7056433	
Affected Version(s): 11.1					
Uncontrolled Resource Consumption	25-Oct-2023	4.9	IBM TXSeries for Multiplatforms, 8.1, 8.2, and 9.1, CICS TX Standard CICS TX Advanced 10.1 and 11.1 could allow a privileged user to cause a denial of service due to uncontrolled resource consumption. IBM X-Force ID: 266016. **CVE ID : CVE-2023-42031**	https://www.ibm.com/support/pages/node/7056429, https://exchange.xforce.ibmcloud.com/vulnerabilities/266061, https://www.ibm.com/support/pages/node/7056433	A-IBM-CICS-241123/729
Product: cognos_dashboards_on_cloud_pak_for_data					
Affected Version(s): 4.7.0					
Cleartext Transmission of Sensitive Information	22-Oct-2023	7.5	IBM Cognos Dashboards on Cloud Pak for Data 4.7.0 exposes sensitive information in container images which could lead to further attacks	https://exchange.xforce.ibmcloud.com/vulnerabilities/260735, https://www.ibm.com/support/pages/node/7031207	A-IBM-COGN-241123/730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			against the system. IBM X-Force ID: 260730. **CVE ID : CVE-2023-38275**		
Cleartext Transmission of Sensitive Information	22-Oct-2023	7.5	IBM Cognos Dashboards on Cloud Pak for Data 4.7.0 exposes sensitive information in environment variables which could aid in further attacks against the system. IBM X-Force ID: 260736. **CVE ID : CVE-2023-38276**	https://exchange.xforce.ibmcloud.com/vulnerabilities/260736, https://www.ibm.com/support/pages/node/7031207	A-IBM-COGN-241123/731
Improper Authentication	22-Oct-2023	6.5	IBM Cognos Dashboards on Cloud Pak for Data 4.7.0 could allow a remote attacker to bypass security restrictions, caused by a reverse tabnabbing flaw. An attacker could exploit this vulnerability and redirect a victim to a phishing site. IBM X-Force ID: 262482. **CVE ID : CVE-2023-38735**	https://www.ibm.com/support/pages/node/7031207, https://exchange.xforce.ibmcloud.com/vulnerabilities/262482	A-IBM-COGN-241123/732
Product: db2					
Affected Version(s): 10.5					
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows	https://exchange.xforce.ibmclou	A-IBM-DB2-241123/733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain databases. IBM X-Force ID: 253440. **CVE ID : CVE-2023-30987**	d.com/vulnerabilities/253440, https://www.ibm.com/support/pages/node/7047560	
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted XML query statement. IBM X-Force ID: 262258. **CVE ID : CVE-2023-38728**	https://exchange.xforce.ibmcloud.com/vulnerabilities/262258, https://www.ibm.com/support/pages/node/7047478	A-IBM-DB2-241123/734
N/A	17-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to denial of service with a specially crafted query containing common table expressions. IBM X-Force ID: 263574. **CVE ID : CVE-2023-40373**	https://www.ibm.com/support/pages/node/7047563, https://exchange.xforce.ibmcloud.com/vulnerabilities/263574	A-IBM-DB2-241123/735
Affected Version(s): 11.1.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain databases. IBM X-Force ID: 253440. **CVE ID : CVE-2023-30987**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253440, https://www.ibm.com/support/pages/node/7047560	A-IBM-DB2-241123/736
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to denial of service with a specially crafted query. IBM X-Force ID: 254037. **CVE ID : CVE-2023-30991**	https://www.ibm.com/support/pages/node/7047499, https://exchange.xforce.ibmcloud.com/vulnerabilities/254037	A-IBM-DB2-241123/737
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 and 11.5 is vulnerable to denial of service with a specially crafted ALTER TABLE statement. IBM X-Force ID: 261616. **CVE ID : CVE-2023-38720**	https://www.ibm.com/support/pages/node/7047489, https://exchange.xforce.ibmcloud.com/vulnerabilities/261616	A-IBM-DB2-241123/738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted XML query statement. IBM X-Force ID: 262258. **CVE ID : CVE-2023-38728**	https://exchange.xforce.ibmcloud.com/vulnerabilities/262258, https://www.ibm.com/support/pages/node/7047478	A-IBM-DB2-241123/739
N/A	17-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to denial of service with a specially crafted query containing common table expressions. IBM X-Force ID: 263574. **CVE ID : CVE-2023-40373**	https://www.ibm.com/support/pages/node/7047563, https://exchange.xforce.ibmcloud.com/vulnerabilities/263574	A-IBM-DB2-241123/740
Affected Version(s): 11.5.8					
N/A	17-Oct-2023	4.4	IBM Db2 11.5 could allow a local user with special privileges to cause a denial of service during database deactivation on DPF. IBM X-Force ID: 261607. **CVE ID : CVE-2023-38719**	https://www.ibm.com/support/pages/node/7047558, https://exchange.xforce.ibmcloud.com/vulnerabilities/261607	A-IBM-DB2-241123/741
Affected Version(s): From (including) 11.5 Up to (excluding) 11.5.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain databases. IBM X-Force ID: 253440. **CVE ID : CVE-2023-30987**	https://exchange.xforce.ibmcloud.com/vulnerabilities/253440, https://www.ibm.com/support/pages/node/7047560	A-IBM-DB2-241123/742
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 and 11.5 is vulnerable to denial of service with a specially crafted ALTER TABLE statement. IBM X-Force ID: 261616. **CVE ID : CVE-2023-38720**	https://www.ibm.com/support/pages/node/7047489, https://exchange.xforce.ibmcloud.com/vulnerabilities/261616	A-IBM-DB2-241123/743
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted XML query statement. IBM X-Force ID: 262258. **CVE ID : CVE-2023-38728**	https://exchange.xforce.ibmcloud.com/vulnerabilities/262258, https://www.ibm.com/support/pages/node/7047478	A-IBM-DB2-241123/744
Affected Version(s): From (including) 11.5 Up to (including) 11.5.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to denial of service with a specially crafted query. IBM X-Force ID: 254037. **CVE ID : CVE-2023-30991**	https://www.ibm.com/support/pages/node/7047499, https://exchange.xforce.ibmcloud.com/vulnerabilities/254037	A-IBM-DB2-241123/745
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX, and Windows (includes Db2 Connect Server) 11.5 is vulnerable to a denial of service with a specially crafted SQL statement. IBM X-Force ID: 262613. **CVE ID : CVE-2023-38740**	https://exchange.xforce.ibmcloud.com/vulnerabilities/262613, https://www.ibm.com/support/pages/node/7047554	A-IBM-DB2-241123/746
N/A	17-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to denial of service with a specially crafted SQL statement using External Tables. IBM X-Force ID: 263499. **CVE ID : CVE-2023-40372**	https://exchange.xforce.ibmcloud.com/vulnerabilities/263499, https://www.ibm.com/support/pages/node/7047561	A-IBM-DB2-241123/747
N/A	17-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows	https://www.ibm.com/support	A-IBM-DB2-241123/748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(includes Db2 Connect Server) is vulnerable to denial of service with a specially crafted query containing common table expressions. IBM X-Force ID: 263574. **CVE ID : CVE-2023-40373**	/pages/node/7047563, https://exchange.xforce.ibmcloud.com/vulnerabilities/263574	
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to denial of service with a specially crafted query statement. IBM X-Force ID: 263575. **CVE ID : CVE-2023-40374**	https://www.ibm.com/support/pages/node/7047261, https://exchange.xforce.ibmcloud.com/vulnerabilities/263575	A-IBM-DB2-241123/749
Product: hardware_management_console					
Affected Version(s): 10.1.1010.0					
Improper Privilege Management	16-Oct-2023	7.8	IBM HMC (Hardware Management Console) 10.1.1010.0 and 10.2.1030.0 could allow a local user to escalate their privileges to root access on a restricted shell. IBM X-Force ID: 260740.	https://exchange.xforce.ibmcloud.com/vulnerabilities/260740, https://www.ibm.com/support/pages/node/7047713	A-IBM-HARD-241123/750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38280		
Affected Version(s): 10.2.1030.0					
Improper Privilege Management	16-Oct-2023	7.8	IBM HMC (Hardware Management Console) 10.1.1010.0 and 10.2.1030.0 could allow a local user to escalate their privileges to root access on a restricted shell. IBM X-Force ID: 260740. **CVE ID : CVE-2023-38280**	https://exchange.xforce.ibmcloud.com/vulnerabilities/260740, https://www.ibm.com/support/pages/node/7047713	A-IBM-HARD-241123/751
Product: qradar_security_information_and_event_manager					
Affected Version(s): 7.5.0					
N/A	29-Oct-2023	4.9	IBM QRadar SIEM 7.5 is vulnerable to information exposure allowing a delegated Admin tenant user with a specific domain security profile assigned to see data from other domains. This vulnerability is due to an incomplete fix for CVE-2022-34352. IBM X-Force ID: 266808. **CVE ID : CVE-2023-43041**	https://www.ibm.com/support/pages/node/7060803, https://exchange.xforce.ibmcloud.com/vulnerabilities/266808	A-IBM-QRAD-241123/752
Product: security_verify_governance					
Affected Version(s): 10.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Oct-2023	8.8	IBM Security Verify Governance 10.0 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 256036. **CVE ID : CVE-2023-33839**	https://exchange.xforce.ibmcloud.com/vulnerabilities/256036, https://www.ibm.com/support/pages/node/7057377	A-IBM-SECU-241123/753
Missing Encryption of Sensitive Data	23-Oct-2023	7.5	IBM Security Verify Governance 10.0 does not encrypt sensitive or critical information before storage or transmission. IBM X-Force ID: 256020. **CVE ID : CVE-2023-33837**	https://www.ibm.com/support/pages/node/7057377, https://exchange.xforce.ibmcloud.com/vulnerabilities/256020	A-IBM-SECU-241123/754
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	4.8	IBM Security Verify Governance 10.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	https://exchange.xforce.ibmcloud.com/vulnerabilities/256037, https://www.ibm.com/support/pages/node/7057377	A-IBM-SECU-241123/755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 256037. **CVE ID : CVE-2023-33840**		
Affected Version(s): 10.0.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Oct-2023	8.8	IBM Security Verify Governance 10.0 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 256036. **CVE ID : CVE-2023-33839**	https://exchange.xforce.ibmcloud.com/vulnerabilities/256036, https://www.ibm.com/support/pages/node/7057377	A-IBM-SECU-241123/756
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	4.8	IBM Security Verify Governance 10.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 256037. **CVE ID : CVE-2023-33840**	https://exchange.xforce.ibmcloud.com/vulnerabilities/256037, https://www.ibm.com/support/pages/node/7057377	A-IBM-SECU-241123/757
Affected Version(s): From (including) 10.0 Up to (excluding) 10.0.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	16-Oct-2023	9.8	IBM Security Verify Governance 10.0 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 256016. **CVE ID : CVE-2023-33836**	https://https://exchange.xforce.ibmcloud.com/vulnerabilities/256016, https://www.ibm.com/support/pages/node/7047640	A-IBM-SECU-241123/758
Unrestricted Upload of File with Dangerous Type	16-Oct-2023	7.2	IBM Security Verify Governance 10.0 could allow a privileged use to upload arbitrary files due to improper file validation. IBM X-Force ID: 259382. **CVE ID : CVE-2023-35018**	https://www.ibm.com/support/pages/node/7050358, https://exchange.xforce.ibmcloud.com/vulnerabilities/259382	A-IBM-SECU-241123/759
Exposure of Resource to Wrong Sphere	16-Oct-2023	4.4	IBM Security Verify Governance 10.0, Identity Manager could allow a local privileged user to obtain sensitive information from source code. IBM X-Force ID: 257769.	https://exchange.xforce.ibmcloud.com/vulnerabilities/257769, https://www.ibm.com/support/pages/node/7050358	A-IBM-SECU-241123/760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35013		
Product: sterling_partner_engagement_manager					
Affected Version(s): 6.1.2					
Missing Authentication for Critical Function	23-Oct-2023	7.5	IBM Sterling Partner Engagement Manager 6.1.2, 6.2.0, and 6.2.2 could allow a remote user to perform unauthorized actions due to improper authentication. IBM X-Force ID: 266896. **CVE ID : CVE-2023-43045**	https://exchange.xforce.ibmcloud.com/vulnerabilities/266896, https://www.ibm.com/support/pages/node/7057409	A-IBM-STER-241123/761
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	5.4	IBM Sterling Partner Engagement Manager 6.1.2, 6.2.0, and 6.2.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 262174.	https://www.ibm.com/support/pages/node/7057407, https://exchange.xforce.ibmcloud.com/vulnerabilities/262174	A-IBM-STER-241123/762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38722		
Affected Version(s): 6.2.0					
Missing Authentication for Critical Function	23-Oct-2023	7.5	IBM Sterling Partner Engagement Manager 6.1.2, 6.2.0, and 6.2.2 could allow a remote user to perform unauthorized actions due to improper authentication. IBM X-Force ID: 266896. **CVE ID : CVE-2023-43045**	https://exchange.xforce.ibmcloud.com/vulnerabilities/266896, https://www.ibm.com/support/pages/node/7057409	A-IBM-STER-241123/763
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	5.4	IBM Sterling Partner Engagement Manager 6.1.2, 6.2.0, and 6.2.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 262174.	https://www.ibm.com/support/pages/node/7057407, https://exchange.xforce.ibmcloud.com/vulnerabilities/262174	A-IBM-STER-241123/764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38722		
Affected Version(s): 6.2.2					
Missing Authentication for Critical Function	23-Oct-2023	7.5	IBM Sterling Partner Engagement Manager 6.1.2, 6.2.0, and 6.2.2 could allow a remote user to perform unauthorized actions due to improper authentication. IBM X-Force ID: 266896. **CVE ID : CVE-2023-43045**	https://exchange.xforce.ibmcloud.com/vulnerabilities/266896, https://www.ibm.com/support/pages/node/7057409	A-IBM-STER-241123/765
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	5.4	IBM Sterling Partner Engagement Manager 6.1.2, 6.2.0, and 6.2.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 262174.	https://www.ibm.com/support/pages/node/7057407, https://exchange.xforce.ibmcloud.com/vulnerabilities/262174	A-IBM-STER-241123/766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38722		
Product: txseries_for_multiplatforms					
Affected Version(s): 8.1					
Uncontrolled Resource Consumption	25-Oct-2023	4.9	IBM TXSeries for Multiplatforms, 8.1, 8.2, and 9.1, CICS TX Standard CICS TX Advanced 10.1 and 11.1 could allow a privileged user to cause a denial of service due to uncontrolled resource consumption. IBM X-Force ID: 266016. **CVE ID : CVE-2023-42031**	https://www.ibm.com/support/pages/node/7056429, https://exchange.xforce.ibmcloud.com/vulnerabilities/266061, https://www.ibm.com/support/pages/node/7056433	A-IBM-TXSE-241123/767
Affected Version(s): 8.2					
Uncontrolled Resource Consumption	25-Oct-2023	4.9	IBM TXSeries for Multiplatforms, 8.1, 8.2, and 9.1, CICS TX Standard CICS TX Advanced 10.1 and 11.1 could allow a privileged user to cause a denial of service due to uncontrolled resource consumption. IBM X-Force ID: 266016. **CVE ID : CVE-2023-42031**	https://www.ibm.com/support/pages/node/7056429, https://exchange.xforce.ibmcloud.com/vulnerabilities/266061, https://www.ibm.com/support/pages/node/7056433	A-IBM-TXSE-241123/768
Affected Version(s): 9.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	25-Oct-2023	4.9	IBM TXSeries for Multiplatforms, 8.1, 8.2, and 9.1, CICS TX Standard CICS TX Advanced 10.1 and 11.1 could allow a privileged user to cause a denial of service due to uncontrolled resource consumption. IBM X-Force ID: 266016. **CVE ID : CVE-2023-42031**	https://www.ibm.com/support/pages/node/7056429, https://exchange.xforce.ibmcloud.com/vulnerabilities/266061, https://www.ibm.com/support/pages/node/7056433	A-IBM-TXSE-241123/769
Product: websphere_application_server_liberty					
Affected Version(s): From (including) 23.0.0.9 Up to (excluding) 23.0.0.11					
Insufficient Session Expiration	25-Oct-2023	9.8	IBM WebSphere Application Server Liberty 23.0.0.9 through 23.0.0.10 could provide weaker than expected security due to improper resource expiration handling. IBM X-Force ID: 268775. **CVE ID : CVE-2023-46158**	https://www.ibm.com/support/pages/node/7058356, https://exchange.xforce.ibmcloud.com/vulnerabilities/268775	A-IBM-WEBS-241123/770
Vendor: icegram					
Product: icegram_express					
Affected Version(s): * Up to (including) 5.6.23					
Improper Limitation of a Pathname to a Restricted	20-Oct-2023	7.2	The Icegram Express plugin for WordPress is vulnerable to Directory Traversal in versions up to,	https://plugins.trac.wordpress.org/browser/email-subscribers/trunk/lite/includes	A-ICE-ICEG-241123/771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			and including, 5.6.23 via the show_es_logs function. This allows administrator-level attackers to read the contents of arbitrary files on the server, which can contain sensitive information including those belonging to other sites, for example in shared hosting environments. **CVE ID : CVE-2023-5414**	/classes/class-email-subscribers-logs.php?rev=2919465#L28	
Vendor: idattend					
Product: idweb					
Affected Version(s): * Up to (excluding) 3.1.053					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	6.1	Reflected cross-site scripting in the StudentSearch component in IDAttend's IDWeb application 3.1.052 and earlier allows hijacking of a user's browsing session by attackers who have convinced the said user to click on a malicious link. **CVE ID : CVE-2023-1356**	N/A	A-IDA-IDWE-241123/772
Affected Version(s): * Up to (including) 3.1.052					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	9.1	Unauthenticated SQL injection in the GetStudentGroupStudents method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers. **CVE ID : CVE-2023-26568**	N/A	A-IDA-IDWE-241123/773
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	9.1	Unauthenticated SQL injection in the StudentPopupDetails_Timetable method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers. **CVE ID : CVE-2023-26569**	N/A	A-IDA-IDWE-241123/774
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	9.1	Unauthenticated SQL injection in the GetExcursionList method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers.	N/A	A-IDA-IDWE-241123/775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26572		
Missing Authentication for Critical Function	25-Oct-2023	9.1	Missing authentication in the SetDB method in IDAttend's IDWeb application 3.1.052 and earlier allows denial of service or theft of database login credentials. **CVE ID : CVE-2023-26573**	N/A	A-IDA-IDWE-241123/776
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	9.1	Unauthenticated SQL injection in the GetVisitors method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers. **CVE ID : CVE-2023-26581**	N/A	A-IDA-IDWE-241123/777
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	9.1	Unauthenticated SQL injection in the GetExcursionDetails method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers. **CVE ID : CVE-2023-26582**	N/A	A-IDA-IDWE-241123/778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	9.1	Unauthenticated SQL injection in the GetCurrentPeriod method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers. **CVE ID : CVE-2023-26583**	N/A	A-IDA-IDWE-241123/779
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	9.1	Unauthenticated SQL injection in the GetStudentInconsistencies method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers. **CVE ID : CVE-2023-26584**	N/A	A-IDA-IDWE-241123/780
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	9.1	Unauthenticated SQL injection in the GetRoomChanges method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers. **CVE ID : CVE-2023-27254**	N/A	A-IDA-IDWE-241123/781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	9.1	Unauthenticated SQL injection in the DeleteRoomChanges method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers. **CVE ID : CVE-2023-27255**	N/A	A-IDA-IDWE-241123/782
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	9.1	Unauthenticated SQL injection in the GetAssignmentsDue method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers. **CVE ID : CVE-2023-27260**	N/A	A-IDA-IDWE-241123/783
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	9.1	Unauthenticated SQL injection in the GetAssignmentsDue method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction or modification of all data by unauthenticated attackers. **CVE ID : CVE-2023-27262**	N/A	A-IDA-IDWE-241123/784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	25-Oct-2023	7.5	Missing authentication in the StudentPopupDetails_Timetable method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction sensitive student data by unauthenticated attackers. **CVE ID : CVE-2023-26570**	N/A	A-IDA-IDWE-241123/785
Missing Authentication for Critical Function	25-Oct-2023	7.5	Missing authentication in the SetStudentNotes method in IDAttend's IDWeb application 3.1.052 and earlier allows modification of student data by unauthenticated attackers. **CVE ID : CVE-2023-26571**	N/A	A-IDA-IDWE-241123/786
Missing Authentication for Critical Function	25-Oct-2023	7.5	Missing authentication in the SearchStudents method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction sensitive student data by unauthenticated attackers. **CVE ID : CVE-2023-26574**	N/A	A-IDA-IDWE-241123/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	25-Oct-2023	7.5	Missing authentication in the SearchStudentsStaff method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction sensitive student and teacher data by unauthenticated attackers. **CVE ID : CVE-2023-26575**	N/A	A-IDA-IDWE-241123/788
Missing Authentication for Critical Function	25-Oct-2023	7.5	Missing authentication in the SearchStudentsRFID method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction sensitive student data by unauthenticated attackers. **CVE ID : CVE-2023-26576**	N/A	A-IDA-IDWE-241123/789
Missing Authentication for Critical Function	25-Oct-2023	7.5	Unauthenticated arbitrary file read in the IDAttend's IDWeb application 3.1.013 allows the retrieval of any file present on the web server by unauthenticated attackers. **CVE ID : CVE-2023-26580**	N/A	A-IDA-IDWE-241123/790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	25-Oct-2023	7.5	Missing authentication in the GetActiveToiletPasses method in IDAttend's IDWeb application 3.1.052 and earlier allows retrieval of student information by unauthenticated attackers. **CVE ID : CVE-2023-27257**	N/A	A-IDA-IDWE-241123/791
Missing Authentication for Critical Function	25-Oct-2023	7.5	Missing authentication in the GetStudentGroupStudents method in IDAttend's IDWeb application 3.1.052 and earlier allows retrieval of student and teacher data by unauthenticated attackers. **CVE ID : CVE-2023-27258**	N/A	A-IDA-IDWE-241123/792
Missing Authentication for Critical Function	25-Oct-2023	7.5	Missing authentication in the GetAssignmentsDue method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction of sensitive student and teacher data by unauthenticated attackers.	N/A	A-IDA-IDWE-241123/793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27259		
Missing Authentication for Critical Function	25-Oct-2023	7.5	Missing authentication in the StudentPopupDetails_ContactDetails method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction of sensitive student data by unauthenticated attackers. **CVE ID : CVE-2023-27375**	N/A	A-IDA-IDWE-241123/794
Missing Authentication for Critical Function	25-Oct-2023	7.5	Missing authentication in the StudentPopupDetails_StudentDetails method in IDAttend's IDWeb application 3.1.052 and earlier allows extraction of sensitive student data by unauthenticated attackers. **CVE ID : CVE-2023-27376**	N/A	A-IDA-IDWE-241123/795
Improper Authentication	25-Oct-2023	7.5	Missing authentication in the StudentPopupDetails_EmergencyContactDetails method in IDAttend's IDWeb	N/A	A-IDA-IDWE-241123/796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application 3.1.052 and earlier allows extraction of sensitive student data by unauthenticated attackers. **CVE ID : CVE-2023-27377**		
Missing Authentication for Critical Function	25-Oct-2023	6.5	Missing authentication in the DeleteAssignments method in IDAttend's IDWeb application 3.1.052 and earlier allows deletion of data by unauthenticated attackers. **CVE ID : CVE-2023-27261**	N/A	A-IDA-IDWE-241123/797
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	Stored cross-site scripting in the IDAttend's IDWeb application 3.1.052 and earlier allows attackers to hijack the browsing session of the logged in user. **CVE ID : CVE-2023-26577**	N/A	A-IDA-IDWE-241123/798
Missing Authentication for Critical Function	25-Oct-2023	5.3	Missing authentication in the GetLogFiles method in IDAttend's IDWeb application 3.1.052 and earlier allows retrieval of sensitive log files	N/A	A-IDA-IDWE-241123/799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by unauthenticated attackers. **CVE ID : CVE-2023-27256**		
Affected Version(s): 3.1.013					
Unrestricted Upload of File with Dangerous Type	25-Oct-2023	8.8	Arbitrary file upload to web root in the IDAttend's IDWeb application 3.1.013 allows authenticated attackers to upload dangerous files to web root such as ASP or ASPX, gaining command execution on the affected server. **CVE ID : CVE-2023-26578**	N/A	A-IDA-IDWE-241123/800
Missing Authentication for Critical Function	25-Oct-2023	5.3	Missing authentication in the DeleteStaff method in IDAttend's IDWeb application 3.1.013 allows deletion of staff information by unauthenticated attackers. **CVE ID : CVE-2023-26579**	N/A	A-IDA-IDWE-241123/801
Vendor: iframe_project					
Product: iframe					
Affected Version(s): * Up to (excluding) 4.7					
Improper Neutralization of Input During Web Page	20-Oct-2023	5.4	The iframe plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `iframe` shortcode	https://www.wordfence.com/threat-intel/vulnerabilities/id/3706ded-55f2-4dfb-	A-IFR-IFRA-241123/802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			in versions up to, and including, 4.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permission and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This was partially patched in version 4.6 and fully patched in version 4.7. **CVE ID : CVE-2023-4919**	bfed-7a14872cd15a?source=cve, https://plugins.trac.wordpress.org/changeset/2970787/iframe#file4	
Vendor: igexsolutions					
Product: wpschoolpress					
Affected Version(s): * Up to (excluding) 2.2.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Oct-2023	8.8	The School Management System WordPress plugin before 2.2.5 uses the WordPress esc_sql() function on a field not delimited by quotes and did not first prepare the query, leading to a SQL injection exploitable by	N/A	A-IGE-WPSC-241123/803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			relatively low-privilege users like Teachers. **CVE ID : CVE-2023-4776**		
Vendor: igorfuna					
Product: ad_inserter					
Affected Version(s): * Up to (including) 2.7.30					
Missing Authorization	19-Oct-2023	5.3	The Ad Inserter for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 2.7.30 via the ai_ajax function. This can allow unauthenticated attackers to extract sensitive data such as post titles and slugs (including those of protected posts along with their passwords), usernames, available roles, the plugin license key provided the remote debugging option is enabled. In the default state it is disabled. **CVE ID : CVE-2023-4645**	https://plugins.trac.wordpress.org/browser/ad-inserter/trunk/ad-inserter.php#L6529	A-IGO-AD_I-241123/804
Vendor: imagely					
Product: nextgen_gallery					
Affected Version(s): * Up to (excluding) 3.39					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Oct-2023	7.5	The WordPress Gallery Plugin WordPress plugin before 3.39 is vulnerable to PHAR Deserialization due to a lack of input parameter validation in the `gallery_edit` function, allowing an attacker to access arbitrary resources on the server. **CVE ID : CVE-2023-3154**	N/A	A-IMA-NEXT-241123/805
Files or Directories Accessible to External Parties	16-Oct-2023	7.2	The WordPress Gallery Plugin WordPress plugin before 3.39 is vulnerable to Arbitrary File Read and Delete due to a lack of input parameter validation in the `gallery_edit` function, allowing an attacker to access arbitrary resources on the server. **CVE ID : CVE-2023-3155**	N/A	A-IMA-NEXT-241123/806
N/A	16-Oct-2023	4.9	The WordPress Gallery Plugin WordPress plugin before 3.39 does not validate some block attributes before using them to generate paths	N/A	A-IMA-NEXT-241123/807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed to include function/s, allowing Admin users to perform LFI attacks **CVE ID : CVE-2023-3279**		
Vendor: info-d-74					
Product: open_street_map					
Affected Version(s): * Up to (including) 1.25					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in InfoD74 WP Open Street Map plugin <= 1.25 versions. **CVE ID : CVE-2023-45645**	N/A	A-INF-OPEN-241123/808
Vendor: inkdrop					
Product: inkdrop					
Affected Version(s): * Up to (excluding) 5.6.0					
Improper Control of Generation of Code ('Code Injection')	30-Oct-2023	7.8	Inkdrop prior to v5.6.0 allows a local attacker to conduct a code injection attack by having a legitimate user open a specially crafted markdown file. **CVE ID : CVE-2023-44141**	N/A	A-INK-INKD-241123/809
Affected Version(s): 5.6.0					
Improper Control of Generation of Code ('Code Injection')	30-Oct-2023	7.8	Inkdrop prior to v5.6.0 allows a local attacker to conduct a code injection attack by having a legitimate	N/A	A-INK-INKD-241123/810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user open a specially crafted markdown file. **CVE ID : CVE-2023-44141**		
Vendor: inohom					
Product: home_manager_gateway					
Affected Version(s): * Up to (excluding) 1.27.12					
N/A	27-Oct-2023	7.5	Improper Protection for Outbound Error Messages and Alert Signals vulnerability in Inohom Home Manager Gateway allows Account Footprinting.This issue affects Home Manager Gateway: before v.1.27.12. **CVE ID : CVE-2023-5570**	N/A	A-INO-HOME-241123/811
Vendor: Insyde					
Product: insydeh2o					
Affected Version(s): 5.2					
N/A	19-Oct-2023	5.3	An issue was discovered in TrEEConfigDriver in Insyde InsydeH2O with kernel 5.0 through 5.5. It can report false TPM PCR values, and thus mask malware activity. Devices use Platform	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2023045	A-INS-INSY-241123/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Configuration Registers (PCRs) to record information about device and software configuration to ensure that the boot process is secure. (For example, Windows uses these PCR measurements to determine device health.) A vulnerable device can masquerade as a healthy device by extending arbitrary values into Platform Configuration Register (PCR) banks. This requires physical access to a target victim's device, or compromise of user credentials for a device. This issue is similar to CVE-2021-42299 (on Surface Pro devices). **CVE ID : CVE-2023-30633**		
Affected Version(s): From (including) 5.3 Up to (excluding) 5.3.05.37.17					
N/A	19-Oct-2023	5.3	An issue was discovered in TrEEConfigDriver in Insyde InsydeH2O with kernel 5.0 through 5.5. It can report	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2023045	A-INS-INSY-241123/813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			false TPM PCR values, and thus mask malware activity. Devices use Platform Configuration Registers (PCRs) to record information about device and software configuration to ensure that the boot process is secure. (For example, Windows uses these PCR measurements to determine device health.) A vulnerable device can masquerade as a healthy device by extending arbitrary values into Platform Configuration Register (PCR) banks. This requires physical access to a target victim's device, or compromise of user credentials for a device. This issue is similar to CVE-2021-42299 (on Surface Pro devices). **CVE ID : CVE-2023-30633**		
Affected Version(s): From (including) 5.4 Up to (excluding) 5.4.05.45.17					
N/A	19-Oct-2023	5.3	An issue was discovered in	https://www.insyde.com/secur	A-INS-INSY-241123/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TrEEConfigDriver in Insyde InsydeH2O with kernel 5.0 through 5.5. It can report false TPM PCR values, and thus mask malware activity. Devices use Platform Configuration Registers (PCRs) to record information about device and software configuration to ensure that the boot process is secure. (For example, Windows uses these PCR measurements to determine device health.) A vulnerable device can masquerade as a healthy device by extending arbitrary values into Platform Configuration Register (PCR) banks. This requires physical access to a target victim's device, or compromise of user credentials for a device. This issue is similar to CVE-2021-42299 (on Surface Pro devices).	ity-pledge, https://www.insyde.com/security-pledge/SA-2023045	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30633		
Affected Version(s): From (including) 5.5 Up to (excluding) 5.5.05.53.17					
N/A	19-Oct-2023	5.3	An issue was discovered in TrEEConfigDriver in Insyde InsydeH2O with kernel 5.0 through 5.5. It can report false TPM PCR values, and thus mask malware activity. Devices use Platform Configuration Registers (PCRs) to record information about device and software configuration to ensure that the boot process is secure. (For example, Windows uses these PCR measurements to determine device health.) A vulnerable device can masquerade as a healthy device by extending arbitrary values into Platform Configuration Register (PCR) banks. This requires physical access to a target victim's device, or compromise of user credentials for	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2023045	A-INS-INSY-241123/815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a device. This issue is similar to CVE-2021-42299 (on Surface Pro devices). **CVE ID : CVE-2023-30633**		
Affected Version(s): From (including) 5.6 Up to (excluding) 5.6.05.60.17					
N/A	19-Oct-2023	5.3	An issue was discovered in TrEEConfigDriver in Insyde InsydeH2O with kernel 5.0 through 5.5. It can report false TPM PCR values, and thus mask malware activity. Devices use Platform Configuration Registers (PCRs) to record information about device and software configuration to ensure that the boot process is secure. (For example, Windows uses these PCR measurements to determine device health.) A vulnerable device can masquerade as a healthy device by extending arbitrary values into Platform Configuration Register (PCR) banks. This	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2023045	A-INS-INSY-241123/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requires physical access to a target victim's device, or compromise of user credentials for a device. This issue is similar to CVE-2021-42299 (on Surface Pro devices). **CVE ID : CVE-2023-30633**		
Vendor: Intelliants					
Product: subrion_cms					
Affected Version(s): 4.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2023	6.1	Multiple Cross-Site Scripting (XSS) vulnerabilities in installation of Subrion CMS v.4.2.1 allows a local attacker to execute arbitrary web scripts via a crafted payload injected into the dbhost, dbname, dbuser, adminusername and adminemail. **CVE ID : CVE-2023-43875**	N/A	A-INT-SUBR-241123/817
Vendor: internetmarketingninjas					
Product: internal_link_building					
Affected Version(s): * Up to (including) 1.2.3					
Cross-Site Request Forgery (CSRF)	25-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Internet Marketing Ninjas Internal Link Building	N/A	A-INT-INTE-241123/818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			plugin <= 1.2.3 versions. **CVE ID : CVE-2023-46193**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Internet Marketing Ninjas Internal Link Building plugin <= 1.2.3 versions. **CVE ID : CVE-2023-46192**	N/A	A-INT-INTE-241123/819
Vendor: ipanorama_360_wordpress_virtual_tour_builder_project					
Product: ipanorama_360_wordpress_virtual_tour_builder					
Affected Version(s): * Up to (including) 1.8.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Oct-2023	6.5	The iPanorama 360 – WordPress Virtual Tour Builder plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 1.8.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with contributor-level and above permissions to	https://plugins.trac.wordpress.org/changeset/2980553/ipanorama-360-virtual-tour-builder-lite#file1, https://plugins.trac.wordpress.org/browser/ipanorama-360-virtual-tour-builder-lite/tags/1.8.0/includes/plugin.php#L439	A-IPA-IPAN-241123/820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-5336**		
Vendor: iptanus					
Product: wordpress_file_upload					
Affected Version(s): * Up to (excluding) 4.23.3					
N/A	16-Oct-2023	5.4	The WordPress File Upload WordPress plugin before 4.23.3 does not sanitise and escape some of its settings, which could allow high privilege users such as contributors to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-4811**	N/A	A-IPT-WORD-241123/821
Vendor: ipushpull					
Product: live_updates_from_excel					
Affected Version(s): * Up to (including) 2.3.2					
N/A	31-Oct-2023	5.4	The Live updates from Excel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ipushpull_page' shortcode in	N/A	A-IPU-LIVE-241123/822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions up to, and including, 2.3.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5116**		
Vendor: ironikus					
Product: wp_mailto_links					
Affected Version(s): * Up to (excluding) 3.1.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	The WP Mailto Links – Protect Email Addresses plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'wpml_mailto' shortcode in versions up to, and including, 3.1.3 due to insufficient input sanitization and output escaping on user supplied attributes.	N/A	A-IRO-WP_M-241123/823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This was partially patched in version 3.1.3 and fully patched in version 3.1.4. **CVE ID : CVE-2023-5109**		
Vendor: iterm2					
Product: iterm2					
Affected Version(s): * Up to (excluding) 3.4.20					
Improper Encoding or Escaping of Output	22-Oct-2023	9.8	iTerm2 before 3.4.20 allow (potentially remote) code execution because of mishandling of certain escape sequences related to tmux integration. **CVE ID : CVE-2023-46300**	https://github.com/gnachman/iTerm2/commit/b2268b03b5f3d4cd8ca275eaef5d16d0fac20009, https://github.com/gnachman/iTerm2/commit/ae8192522661c34d1cbe57f6f9ef2ff0a337c2a5	A-ITE-ITER-241123/824
Improper Encoding or Escaping of Output	22-Oct-2023	9.8	iTerm2 before 3.4.20 allow (potentially remote) code execution because of mishandling of	https://github.com/gnachman/iTerm2/commit/b2268b03b5f3d4cd8ca275eaef5d16d0fac2000	A-ITE-ITER-241123/825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			certain escape sequences related to upload. **CVE ID : CVE-2023-46301**	9, https://github.com/gnachman/iTerm2/commit/85cbf5ebda472c9ec295887e99c2b6f1b5867f1b	
Affected Version(s): * Up to (including) 3.4.21					
N/A	23-Oct-2023	9.8	iTermSessionLauncher.m in iTerm2 before 3.5.0beta12 does not sanitize paths in x-man-page URLs. They may have shell metacharacters for a /usr/bin/man command line. **CVE ID : CVE-2023-46321**	https://iterm2.com/downloads.html	A-ITE-ITER-241123/826
N/A	23-Oct-2023	9.8	iTermSessionLauncher.m in iTerm2 before 3.5.0beta12 does not sanitize ssh hostnames in URLs. The hostname's initial character may be non-alphanumeric. The hostname's other characters may be outside the set of alphanumeric characters, dash, and period. **CVE ID : CVE-2023-46322**	https://iterm2.com/downloads.html	A-ITE-ITER-241123/827
Affected Version(s): 3.5.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Oct-2023	9.8	iTermSessionLauncher.m in iTerm2 before 3.5.0beta12 does not sanitize paths in x-man-page URLs. They may have shell metacharacters for a /usr/bin/man command line. **CVE ID : CVE-2023-46321**	https://iterm2.com/downloads.html	A-ITE-ITER-241123/828
N/A	23-Oct-2023	9.8	iTermSessionLauncher.m in iTerm2 before 3.5.0beta12 does not sanitize ssh hostnames in URLs. The hostname's initial character may be non-alphanumeric. The hostname's other characters may be outside the set of alphanumeric characters, dash, and period. **CVE ID : CVE-2023-46322**	https://iterm2.com/downloads.html	A-ITE-ITER-241123/829
Vendor: ivanti					
Product: endpoint_manager					
Affected Version(s): * Up to (excluding) 2022					
Deserialization of Untrusted Data	18-Oct-2023	9.8	Unsafe Deserialization of User Input could lead to Execution of Unauthorized Operations in Ivanti Endpoint Manager 2022 su3 and all previous	https://forums.ivanti.com/s/article/SA-2023-08-08-CVE-2023-35084?language=en_US	A-IVA-ENDP-241123/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions, which could allow an attacker to execute commands remotely. **CVE ID : CVE-2023-35084**		
N/A	18-Oct-2023	6.5	Allows an authenticated attacker with network access to read arbitrary files on Endpoint Manager recently discovered on 2022 SU3 and all previous versions potentially leading to the leakage of sensitive information. **CVE ID : CVE-2023-35083**	https://forums.ivanti.com/s/article/SA-2023-06-20-CVE-2023-35083?language=en_US	A-IVA-ENDP-241123/831
Affected Version(s): 2022					
Deserialization of Untrusted Data	18-Oct-2023	9.8	Unsafe Deserialization of User Input could lead to Execution of Unauthorized Operations in Ivanti Endpoint Manager 2022 su3 and all previous versions, which could allow an attacker to execute commands remotely. **CVE ID : CVE-2023-35084**	https://forums.ivanti.com/s/article/SA-2023-08-08-CVE-2023-35084?language=en_US	A-IVA-ENDP-241123/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	6.5	Allows an authenticated attacker with network access to read arbitrary files on Endpoint Manager recently discovered on 2022 SU3 and all previous versions potentially leading to the leakage of sensitive information. **CVE ID : CVE-2023-35083**	https://forums.ivanti.com/s/article/SA-2023-06-20-CVE-2023-35083?language=en_US	A-IVA-ENDP-241123/833
Product: secure_access_client					
Affected Version(s): * Up to (excluding) 22.6					
Time-of-check Time-of-use (TOCTOU) Race Condition	25-Oct-2023	7	A logged in user may elevate its permissions by abusing a Time-of-Check to Time-of-Use (TOCTOU) race condition. When a particular process flow is initiated, an attacker can exploit this condition to gain unauthorized elevated privileges on the affected system. **CVE ID : CVE-2023-38041**	https://forums.ivanti.com/s/article/CVE-2023-38041-New-client-side-release-to-address-a-privilege-escalation-on-Windows-user-machines?language=en_US	A-IVA-SECU-241123/834
Vendor: ixpdata					
Product: easyinstall					
Affected Version(s): 6.6.14884.0					
N/A	19-Oct-2023	7.8	An issue discovered in IXP	N/A	A-IXP-EASY-241123/835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Data Easy Install v.6.6.14884.0 allows local attackers to gain escalated privileges via weak encoding of sensitive information. **CVE ID : CVE-2023-27793**		
Affected Version(s): 6.6.148840					
N/A	19-Oct-2023	9.8	An issue discovered in IXP EasyInstall 6.6.14884.0 allows attackers to run arbitrary commands, gain escalated privilege, and cause other unspecified impacts via unauthenticated API calls. **CVE ID : CVE-2023-30131**	N/A	A-IXP-EASY-241123/836
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	19-Oct-2023	8.1	An issue found in IXP Data Easy Install 6.6.148840 allows a remote attacker to escalate privileges via insecure PRNG. **CVE ID : CVE-2023-27791**	N/A	A-IXP-EASY-241123/837
Missing Authorization	19-Oct-2023	7.8	An issue found in IXP Data Easy Install v.6.6.14884.0 allows an attacker to escalate	N/A	A-IXP-EASY-241123/838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges via lack of permissions applied to sub directories. **CVE ID : CVE-2023-27792**		
N/A	19-Oct-2023	7.8	An issue found in IXP Data Easy Install v.6.6.14884.0 allows a local attacker to gain privileges via a static XOR key. **CVE ID : CVE-2023-27795**	N/A	A-IXP-EASY-241123/839
Affected Version(s): 6.6.14907.0					
Inadequate Encryption Strength	19-Oct-2023	7.8	An issue discovered in IXP Data EasyInstall 6.6.14907.0 allows attackers to gain escalated privileges via static Cryptographic Key. **CVE ID : CVE-2023-30132**	N/A	A-IXP-EASY-241123/840
Vendor: Jenkins					
Product: cloudbees_cd					
Affected Version(s): * Up to (including) 1.1.32					
Improper Link Resolution Before File Access ('Link Following')	25-Oct-2023	8.1	Jenkins CloudBees CD Plugin 1.1.32 and earlier follows symbolic links to locations outside of the expected directory during the cleanup process of the 'CloudBees CD - Publish Artifact'	https://www.jenkins.io/security/advisory/2023-10-25/#SECURITY-3237	A-JEN-CLOU-241123/841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			post-build step, allowing attackers able to configure jobs to delete arbitrary files on the Jenkins controller file system. **CVE ID : CVE-2023-46654**		
Improper Link Resolution Before File Access ('Link Following')	25-Oct-2023	6.5	Jenkins CloudBees CD Plugin 1.1.32 and earlier follows symbolic links to locations outside of the directory from which artifacts are published during the 'CloudBees CD - Publish Artifact' post-build step, allowing attackers able to configure jobs to publish arbitrary files from the Jenkins controller file system to the previously configured CloudBees CD server. **CVE ID : CVE-2023-46655**	https://www.jenkins.io/security/advisory/2023-10-25/#SECURITY-3238	A-JEN-CLOU-241123/842
Product: edgewall_trac					
Affected Version(s): * Up to (including) 1.13					
Improper Neutralization of Input During Web Page	25-Oct-2023	5.4	Jenkins Edgewall Trac Plugin 1.13 and earlier does not escape the Trac website URL on the build page,	https://www.jenkins.io/security/advisory/2023-10-25/#SECURITY-3247	A-JEN-EDGE-241123/843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission. **CVE ID : CVE-2023-46659**		
Product: github					
Affected Version(s): * Up to (including) 1.37.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	Jenkins GitHub Plugin 1.37.3 and earlier does not escape the GitHub project URL on the build page when showing changes, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission. **CVE ID : CVE-2023-46650**	https://www.jenkins.io/security/advisory/2023-10-25/#SECURITY-3246	A-JEN-GITH-241123/844
Product: gogs					
Affected Version(s): * Up to (including) 1.0.15					
Incorrect Comparison	25-Oct-2023	5.3	Jenkins Gogs Plugin 1.0.15 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal,	https://www.jenkins.io/security/advisory/2023-10-25/#SECURITY-2896	A-JEN-GOGS-241123/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially allowing attackers to use statistical methods to obtain a valid webhook token. **CVE ID : CVE-2023-46657**		
Product: lambdatest-automation					
Affected Version(s): * Up to (excluding) 1.21.0					
Cleartext Storage of Sensitive Information	25-Oct-2023	6.5	Jenkins lambdatest-automation Plugin 1.20.10 and earlier logs LAMBDATEST Credentials access token at the INFO level, potentially resulting in its exposure. **CVE ID : CVE-2023-46653**	https://www.jenkins.io/security/advisory/2023-10-25/#SECURITY-3202	A-JEN-LAMB-241123/846
Affected Version(s): * Up to (including) 1.20.9					
Missing Authorization	25-Oct-2023	4.3	A missing permission check in Jenkins lambdatest-automation Plugin 1.20.9 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of LAMBDATEST credentials stored in Jenkins. **CVE ID : CVE-2023-46652**	https://www.jenkins.io/security/advisory/2023-10-25/#SECURITY-3222	A-JEN-LAMB-241123/847
Product: msteams_webhook_trigger					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 0.1.0					
Incorrect Comparison	25-Oct-2023	5.3	Jenkins MSTeams Webhook Trigger Plugin 0.1.1 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token. **CVE ID : CVE-2023-46658**	https://www.jenkins.io/security/advisory/2023-10-25/#SECURITY-2876	A-JEN-MSTE-241123/848
Affected Version(s): 0.1.1					
Incorrect Comparison	25-Oct-2023	5.3	Jenkins MSTeams Webhook Trigger Plugin 0.1.1 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token. **CVE ID : CVE-2023-46658**	https://www.jenkins.io/security/advisory/2023-10-25/#SECURITY-2876	A-JEN-MSTE-241123/849
Product: multibranch_scan_webhook_trigger					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.0.9					
Incorrect Comparison	25-Oct-2023	5.3	Jenkins Multibranch Scan Webhook Trigger Plugin 1.0.9 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token. **CVE ID : CVE-2023-46656**	https://www.jenkins.io/security/advisory/2023-10-25/#SECURITY-2875	A-JEN-MULT-241123/850
Product: warnings					
Affected Version(s): * Up to (including) 10.5.0					
Insufficiently Protected Credentials	25-Oct-2023	6.5	Jenkins Warnings Plugin 10.5.0 and earlier does not set the appropriate context for credentials lookup, allowing attackers with Item/Configure permission to access and capture credentials they are not entitled to. This fix has been backported to 10.4.1. **CVE ID : CVE-2023-46651**	https://www.jenkins.io/security/advisory/2023-10-25/#SECURITY-3265	A-JEN-WARN-241123/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: zanata					
Affected Version(s): * Up to (including) 0.6					
Incorrect Comparison	25-Oct-2023	5.3	Jenkins Zanata Plugin 0.6 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token hashes are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token. **CVE ID : CVE-2023-46660**	https://www.jenkins.io/security/advisory/2023-10-25/#SECURITY-2879	A-JEN-ZANA-241123/852
Vendor: joovii					
Product: sendle_shipping					
Affected Version(s): * Up to (including) 5.13					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Joovii Sendle Shipping Plugin plugin <= 5.13 versions. **CVE ID : CVE-2023-45761**	N/A	A-JOO-SEND-241123/853
Vendor: jorani					
Product: leave_management_system					
Affected Version(s): 1.0.3					
Improper Neutralization of Special Elements	16-Oct-2023	6.5	An issue in Jorani Leave Management System 1.0.3 allows a remote attacker to execute	N/A	A-JOR-LEAV-241123/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
in Output Used by a Downstream Component ('Injection')			arbitrary HTML code via a crafted script to the comment field of the List of Leave requests page. **CVE ID : CVE-2023-45540**		
Vendor: jose4j_project					
Product: jose4j					
Affected Version(s): * Up to (excluding) 0.9.3					
Insufficient Entropy	25-Oct-2023	7.5	jose4j before v0.9.3 allows attackers to set a low iteration count of 1000 or less. **CVE ID : CVE-2023-31582**	N/A	A-JOS-JOSE-241123/855
Vendor: jtekt					
Product: onsinview2					
Affected Version(s): * Up to (including) 2.0.1					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Oct-2023	7.8	Improper restriction of operations within the bounds of a memory buffer issue exists in OnSinView2 versions 2.0.1 and earlier. If this vulnerability is exploited, information may be disclosed or arbitrary code may be executed by having a user open a specially crafted OnSinView2 project file.	https://www.electronics.jtekt.co.jp/en/topics/202310175488/	A-JTE-ONSI-241123/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-42506		
Out-of-bounds Write	17-Oct-2023	7.8	Stack-based buffer overflow vulnerability exists in OnSinView2 versions 2.0.1 and earlier. If this vulnerability is exploited, information may be disclosed or arbitrary code may be executed by having a user open a specially crafted OnSinView2 project file. **CVE ID : CVE-2023-42507**	https://www.electronics.jtekt.co.jp/en/topics/202310175488/	A-JTE-ONSI-241123/857
Vendor: Justsystems					
Product: easy_postcard_max					
Affected Version(s): -					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability.	N/A	A-JUS-EASY-241123/858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34366		
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**	N/A	A-JUS-EASY-241123/859
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later	N/A	A-JUS-EASY-241123/860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow for memory corruption, potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**		
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**	N/A	A-JUS-EASY-241123/861
Product: ichitaro_2021					
Affected Version(s): -					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of	N/A	A-JUS-ICHI-241123/862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ichitaro 2023 1.0.1.59372. A specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34366**		
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**	N/A	A-JUS-ICHI-241123/863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption, potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**	N/A	A-JUS-ICHI-241123/864
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can	N/A	A-JUS-ICHI-241123/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**		
Product: ichitaro_2022					
Affected Version(s): -					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34366**	N/A	A-JUS-ICHI-241123/866
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A	N/A	A-JUS-ICHI-241123/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**		
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption, potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**	N/A	A-JUS-ICHI-241123/868
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of	N/A	A-JUS-ICHI-241123/869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**		
Product: ichitaro_2023					
Affected Version(s): 1.0.1.59372					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34366**	N/A	A-JUS-ICHI-241123/870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**	N/A	A-JUS-ICHI-241123/871
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption,	N/A	A-JUS-ICHI-241123/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**		
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**	N/A	A-JUS-ICHI-241123/873
Product: ichitaro_government_10					
Affected Version(s): -					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A	N/A	A-JUS-ICHI-241123/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34366**		
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**	N/A	A-JUS-ICHI-241123/875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption, potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**	N/A	A-JUS-ICHI-241123/876
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can	N/A	A-JUS-ICHI-241123/877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**		
Product: ichitaro_government_8					
Affected Version(s): -					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34366**	N/A	A-JUS-ICHI-241123/878
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A	N/A	A-JUS-ICHI-241123/879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**		
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption, potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**	N/A	A-JUS-ICHI-241123/880
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of	N/A	A-JUS-ICHI-241123/881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**		
Product: ichitaro_government_9					
Affected Version(s): -					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34366**	N/A	A-JUS-ICHI-241123/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**	N/A	A-JUS-ICHI-241123/883
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption,	N/A	A-JUS-ICHI-241123/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**		
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**	N/A	A-JUS-ICHI-241123/885
Product: ichitaro_pro_3					
Affected Version(s): -					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A	N/A	A-JUS-ICHI-241123/886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34366**		
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**	N/A	A-JUS-ICHI-241123/887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption, potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**	N/A	A-JUS-ICHI-241123/888
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can	N/A	A-JUS-ICHI-241123/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**		
Product: ichitaro_pro_4					
Affected Version(s): -					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34366**	N/A	A-JUS-ICHI-241123/890
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A	N/A	A-JUS-ICHI-241123/891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**		
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption, potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**	N/A	A-JUS-ICHI-241123/892
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of	N/A	A-JUS-ICHI-241123/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**		
Product: ichitaro_pro_5					
Affected Version(s): -					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34366**	N/A	A-JUS-ICHI-241123/894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**	N/A	A-JUS-ICHI-241123/895
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption,	N/A	A-JUS-ICHI-241123/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**		
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**	N/A	A-JUS-ICHI-241123/897
Product: just_government_3					
Affected Version(s): -					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A	N/A	A-JUS-JUST-241123/898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34366**		
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**	N/A	A-JUS-JUST-241123/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption, potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**	N/A	A-JUS-JUST-241123/900
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can	N/A	A-JUS-JUST-241123/901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**		
Product: just_government_4					
Affected Version(s): -					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34366**	N/A	A-JUS-JUST-241123/902
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A	N/A	A-JUS-JUST-241123/903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**		
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption, potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**	N/A	A-JUS-JUST-241123/904
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of	N/A	A-JUS-JUST-241123/905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**		
Product: just_government_5					
Affected Version(s): -					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34366**	N/A	A-JUS-JUST-241123/906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**	N/A	A-JUS-JUST-241123/907
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption,	N/A	A-JUS-JUST-241123/908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**		
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**	N/A	A-JUS-JUST-241123/909
Product: just_office_3					
Affected Version(s): -					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A	N/A	A-JUS-JUST-241123/910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34366**		
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**	N/A	A-JUS-JUST-241123/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption, potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**	N/A	A-JUS-JUST-241123/912
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can	N/A	A-JUS-JUST-241123/913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**		
Product: just_office_4					
Affected Version(s): -					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34366**	N/A	A-JUS-JUST-241123/914
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A	N/A	A-JUS-JUST-241123/915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**		
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption, potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**	N/A	A-JUS-JUST-241123/916
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of	N/A	A-JUS-JUST-241123/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**		
Product: just_office_5					
Affected Version(s): -					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34366**	N/A	A-JUS-JUST-241123/918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**	N/A	A-JUS-JUST-241123/919
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption,	N/A	A-JUS-JUST-241123/920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**		
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**	N/A	A-JUS-JUST-241123/921
Product: just_police_3					
Affected Version(s): -					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A	N/A	A-JUS-JUST-241123/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34366**		
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**	N/A	A-JUS-JUST-241123/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption, potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**	N/A	A-JUS-JUST-241123/924
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can	N/A	A-JUS-JUST-241123/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**		
Product: just_police_4					
Affected Version(s): -					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34366**	N/A	A-JUS-JUST-241123/926
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A	N/A	A-JUS-JUST-241123/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**		
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption, potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**	N/A	A-JUS-JUST-241123/928
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of	N/A	A-JUS-JUST-241123/929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**		
Product: just_police_5					
Affected Version(s): -					
Use After Free	19-Oct-2023	7.8	A use-after-free vulnerability exists in the Figure stream parsing functionality of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause memory corruption, resulting in arbitrary code execution. Victim would need to open a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-34366**	N/A	A-JUS-JUST-241123/930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists within the parsers for both the "DocumentViewStyles" and "DocumentEditStyles" streams of Ichitaro 2023 1.0.1.59372 when processing types 0x0000-0x0009 of a style record with the type 0x2008. A specially crafted document can cause memory corruption, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-35126**	N/A	A-JUS-JUST-241123/931
Integer Overflow or Wraparound	19-Oct-2023	7.8	An integer overflow exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause the parser to make an under-sized allocation, which can later allow for memory corruption,	N/A	A-JUS-JUST-241123/932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially resulting in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38127**		
Out-of-bounds Write	19-Oct-2023	7.8	An out-of-bounds write vulnerability exists in the "HyperLinkFrame" stream parser of Ichitaro 2023 1.0.1.59372. A specially crafted document can cause a type confusion, which can lead to memory corruption and eventually arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-38128**	N/A	A-JUS-JUST-241123/933
Vendor: juzaweb					
Product: cms					
Affected Version(s): * Up to (including) 3.4					
Improper Neutralization of Special Elements in Output	28-Oct-2023	7.8	An issue in juzawebCMS v.3.4 and before allows a remote attacker to execute arbitrary code via a crafted	N/A	A-JUZ-CMS-241123/934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Used by a Downstream Component ('Injection')			file to the custom plugin function. **CVE ID : CVE-2023-46468**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Oct-2023	5.4	Cross Site Scripting vulnerability in juzawebCMS v.3.4 and before allows a remote attacker to execute arbitrary code via a crafted payload to the username parameter of the registration page. **CVE ID : CVE-2023-46467**	N/A	A-JUZ-CMS-241123/935
Vendor: katieseaborn					
Product: zotpress					
Affected Version(s): * Up to (excluding) 7.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Katie Seaborn Zotpress plugin <= 7.3.4 versions. **CVE ID : CVE-2023-46313**	N/A	A-KAT-ZOTP-241123/936
Vendor: kevinweber					
Product: lazy_load_for_videos					
Affected Version(s): * Up to (including) 2.18.2					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Kevin Weber Lazy Load for Videos	N/A	A-KEV-LAZY-241123/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			plugin <= 2.18.2 versions. **CVE ID : CVE-2023-45656**		
Vendor: knowband					
Product: supercheckout					
Affected Version(s): From (including) 5.0.7 Up to (excluding) 6.0.7					
Unrestricted Upload of File with Dangerous Type	19-Oct-2023	9.8	KnowBand supercheckout > 5.0.7 and < 6.0.7 is vulnerable to Unrestricted Upload of File with Dangerous Type. In the module "Module One Page Checkout, Social Login & Mailchimp" (supercheckout), a guest can upload files with extensions .php **CVE ID : CVE-2023-45384**	N/A	A-KNO-SUPE-241123/938
Vendor: kochm					
Product: mendeley_plugin					
Affected Version(s): * Up to (including) 1.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Michael Koch Mendeley Plugin plugin <= 1.3.2 versions. **CVE ID : CVE-2023-45073**	N/A	A-KOC-MEND-241123/939
Vendor: kodcloud					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: kodbox					
Affected Version(s): 1.44					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	5.4	kodbox 1.44 is vulnerable to Cross Site Scripting (XSS). Customizing global HTML results in storing XSS. **CVE ID : CVE-2023-45998**	N/A	A-KOD-KODB-241123/940
Vendor: Kubernetes					
Product: ingress-nginx					
Affected Version(s): * Up to (excluding) 1.9.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	25-Oct-2023	8.8	Ingress nginx annotation injection causes arbitrary command execution. **CVE ID : CVE-2023-5043**	https://github.com/kubernetes/ingress-nginx/issues/10571	A-KUB-INGR-241123/941
Improper Control of Generation of Code ('Code Injection')	25-Oct-2023	8.8	Code injection via nginx.ingress.kubernetes.io/permanent-redirect annotation. **CVE ID : CVE-2023-5044**	https://github.com/kubernetes/ingress-nginx/issues/10572	A-KUB-INGR-241123/942
Vendor: langchain					
Product: langchain					
Affected Version(s): * Up to (excluding) 0.0.317					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	19-Oct-2023	8.8	LangChain before 0.0.317 allows SSRF via document_loaders/recursive_url_loader.py because crawling can proceed from an external server to an internal server. **CVE ID : CVE-2023-46229**	https://github.com/langchain-ai/langchain/commit/9ecb7240a480720ec9d739b3877a52f76098a2b8, https://github.com/langchain-ai/langchain/pull/11925	A-LAN-LANG-241123/943
Affected Version(s): * Up to (including) 0.0.155					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Oct-2023	9.8	In Langchain through 0.0.155, prompt injection allows execution of arbitrary code against the SQL service provided by the chain. **CVE ID : CVE-2023-32785**	N/A	A-LAN-LANG-241123/944
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Oct-2023	7.5	In Langchain through 0.0.155, prompt injection allows an attacker to force the service to retrieve data from an arbitrary URL, essentially providing SSRF and potentially injecting content into downstream tasks. **CVE ID : CVE-2023-32786**	N/A	A-LAN-LANG-241123/945
Vendor: lava-code					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: lava_directory_manager					
Affected Version(s): * Up to (including) 1.1.34					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2023	6.1	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Lavacode Lava Directory Manager plugin <= 1.1.34 versions. **CVE ID : CVE-2023-46081**	N/A	A-LAV-LAVA-241123/946
Vendor: lcdf					
Product: gifsicle					
Affected Version(s): 1.94					
Incorrect Comparison	18-Oct-2023	7.8	gifsicle-1.94 was found to have a floating point exception (FPE) vulnerability via resize_stream at src/xform.c. **CVE ID : CVE-2023-46009**	https://github.com/kohler/gifsicle/issues/196	A-LCD-GIFS-241123/947
Vendor: leadsquared					
Product: leadsquared_suite					
Affected Version(s): * Up to (including) 0.7.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in LeadSquared Suite plugin <= 0.7.4 versions. **CVE ID : CVE-2023-45833**	N/A	A-LEA-LEAD-241123/948
Vendor: leantime					
Product: leantime					
Affected Version(s): * Up to (excluding) 2.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Oct-2023	6.5	Leantime is an open source project management system. A 'userId' variable in `app/domain/files/repositories/class.files.php` is not parameterized. An authenticated attacker can send a carefully crafted POST request to `/api/jsonrpc` to exploit an SQL injection vulnerability. Confidentiality is impacted as it allows for dumping information from the database. This issue has been addressed in version 2.4-beta-4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45826**	https://github.com/Leantime/leantime/commit/be75f1e0f311d11c00a0bdc7079a62eef3594bf0, https://github.com/Leantime/leantime/security/advisories/GHSA-559g-3h98-g3fj	A-LEA-LEAN-241123/949
Affected Version(s): 2.4					
Improper Neutralization of Special Elements used in an SQL Command	19-Oct-2023	6.5	Leantime is an open source project management system. A 'userId' variable in `app/domain/files/repositories/class.files.php` is not	https://github.com/Leantime/leantime/commit/be75f1e0f311d11c00a0bdc7079a62eef3594bf0, https://github.com/Leantime/l	A-LEA-LEAN-241123/950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			parameterized. An authenticated attacker can send a carefully crafted POST request to `/api/jsonrpc` to exploit an SQL injection vulnerability. Confidentiality is impacted as it allows for dumping information from the database. This issue has been addressed in version 2.4-beta-4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45826**	eantime/security/advisories/GHSA-559g-3h98-g3fj	
Vendor: learndash					
Product: learndash					
Affected Version(s): * Up to (including) 4.5.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	31-Oct-2023	8.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LearnDash LearnDash LMS allows SQL Injection.This issue affects LearnDash LMS: from n/a through 4.5.3.	N/A	A-LEA-LEAR-241123/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28777		
Vendor: librenms					
Product: librenms					
Affected Version(s): * Up to (including) 23.9.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Oct-2023	6.5	SQL Injection in GitHub repository librenms/librenms prior to 23.10.0. **CVE ID : CVE-2023-5591**	https://github.com/librenms/librenms/commit/908aef65967ce6184bdc587fd105660d5d55129e	A-LIB-LIBR-241123/952
Vendor: libsyn					
Product: libsyn_publisher_hub					
Affected Version(s): * Up to (including) 1.4.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Libsyn Libsyn Publisher Hub plugin <= 1.4.4 versions. **CVE ID : CVE-2023-45835**	N/A	A-LIB-LIBS-241123/953
Vendor: Liferay					
Product: digital_experience_platform					
Affected Version(s): 7.2					
Improper Neutralization of Input During Web Page Generation	17-Oct-2023	5.4	Stored cross-site scripting (XSS) vulnerability in the Wiki widget in Liferay Portal 7.1.0 through 7.4.3.87, and Liferay DXP 7.0 fix pack 83 through	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-42628	A-LIF-DIGI-241123/954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			102, 7.1 fix pack 28 and earlier, 7.2 fix pack 20 and earlier, 7.3 update 33 and earlier, and 7.4 before update 88 allows remote attackers to inject arbitrary web script or HTML into a parent wiki page via a crafted payload injected into a wiki page's 'Content' text field. **CVE ID : CVE-2023-42628**		
Affected Version(s): 7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	5.4	Stored cross-site scripting (XSS) vulnerability in the Wiki widget in Liferay Portal 7.1.0 through 7.4.3.87, and Liferay DXP 7.0 fix pack 83 through 102, 7.1 fix pack 28 and earlier, 7.2 fix pack 20 and earlier, 7.3 update 33 and earlier, and 7.4 before update 88 allows remote attackers to inject arbitrary web script or HTML into a parent wiki page via a crafted payload injected into a wiki page's 'Content' text field.	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-42628	A-LIF-DIGI-241123/955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-42628		
Affected Version(s): 7.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	5.4	Stored cross-site scripting (XSS) vulnerability in the Wiki widget in Liferay Portal 7.1.0 through 7.4.3.87, and Liferay DXP 7.0 fix pack 83 through 102, 7.1 fix pack 28 and earlier, 7.2 fix pack 20 and earlier, 7.3 update 33 and earlier, and 7.4 before update 88 allows remote attackers to inject arbitrary web script or HTML into a parent wiki page via a crafted payload injected into a wiki page's 'Content' text field. **CVE ID : CVE-2023-42628**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-42628	A-LIF-DIGI-241123/956
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	5.4	Stored cross-site scripting (XSS) vulnerability in Page Tree menu Liferay Portal 7.3.6 through 7.4.3.78, and Liferay DXP 7.3 fix pack 1 through update 23, and 7.4 before update 79 allows remote attackers to inject arbitrary web script or HTML via a crafted payload	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-44310	A-LIF-DIGI-241123/957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injected into page's "Name" text field. **CVE ID : CVE-2023-44310**		
Affected Version(s): 7.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	5.4	Multiple stored cross-site scripting (XSS) vulnerabilities in the Commerce module in Liferay Portal 7.3.5 through 7.4.3.91, and Liferay DXP 7.3 update 33 and earlier, and 7.4 before update 92 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a (1) Shipping Name, (2) Shipping Phone Number, (3) Shipping Address, (4) Shipping Address 2, (5) Shipping Address 3, (6) Shipping Zip, (7) Shipping City, (8) Shipping Region (9), Shipping Country, (10) Billing Name, (11) Billing Phone Number, (12) Billing Address, (13) Billing Address 2, (14) Billing Address 3, (15) Billing Zip,	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-42627	A-LIF-DIGI-241123/958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(16) Billing City, (17) Billing Region, (18) Billing Country, or (19) Region Code. **CVE ID : CVE-2023-42627**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	5.4	Stored cross-site scripting (XSS) vulnerability in the Wiki widget in Liferay Portal 7.1.0 through 7.4.3.87, and Liferay DXP 7.0 fix pack 83 through 102, 7.1 fix pack 28 and earlier, 7.2 fix pack 20 and earlier, 7.3 update 33 and earlier, and 7.4 before update 88 allows remote attackers to inject arbitrary web script or HTML into a parent wiki page via a crafted payload injected into a wiki page's 'Content' text field. **CVE ID : CVE-2023-42628**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-42628	A-LIF-DIGI-241123/959
Affected Version(s): 7.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	6.1	Reflected cross-site scripting (XSS) vulnerability on the Export for Translation page in Liferay Portal 7.4.3.4 through 7.4.3.85, and Liferay DXP 7.4	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-42497	A-LIF-DIGI-241123/960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before update 86 allows remote attackers to inject arbitrary web script or HTML via the `_com_liferay_translation_web_internal_portlet_TranslationPortlet_redirect` parameter. **CVE ID : CVE-2023-42497**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities in the Plugin for OAuth 2.0 module's OAuth2ProviderApplicationRedirect class in Liferay Portal 7.4.3.41 through 7.4.3.89, and Liferay DXP 7.4 update 41 through update 89 allow remote attackers to inject arbitrary web script or HTML via the (1) code, or (2) error parameter. This issue is caused by an incomplete fix in CVE-2023-33941. **CVE ID : CVE-2023-44311**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-44311	A-LIF-DIGI-241123/961
Improper Neutralization of	17-Oct-2023	5.4	Multiple stored cross-site scripting (XSS)	https://liferay.dev/portal/security/known-	A-LIF-DIGI-241123/962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			vulnerabilities in the Commerce module in Liferay Portal 7.3.5 through 7.4.3.91, and Liferay DXP 7.3 update 33 and earlier, and 7.4 before update 92 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a (1) Shipping Name, (2) Shipping Phone Number, (3) Shipping Address, (4) Shipping Address 2, (5) Shipping Address 3, (6) Shipping Zip, (7) Shipping City, (8) Shipping Region (9), Shipping Country, (10) Billing Name, (11) Billing Phone Number, (12) Billing Address, (13) Billing Address 2, (14) Billing Address 3, (15) Billing Zip, (16) Billing City, (17) Billing Region, (18) Billing Country, or (19) Region Code. **CVE ID : CVE-2023-42627**	vulnerabilities/-/asset_publisher/jekt/content/cve-2023-42627	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	5.4	Stored cross-site scripting (XSS) vulnerability in the Wiki widget in Liferay Portal 7.1.0 through 7.4.3.87, and Liferay DXP 7.0 fix pack 83 through 102, 7.1 fix pack 28 and earlier, 7.2 fix pack 20 and earlier, 7.3 update 33 and earlier, and 7.4 before update 88 allows remote attackers to inject arbitrary web script or HTML into a parent wiki page via a crafted payload injected into a wiki page's 'Content' text field. **CVE ID : CVE-2023-42628**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-42628	A-LIF-DIGI-241123/963
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	5.4	Stored cross-site scripting (XSS) vulnerability in the manage vocabulary page in Liferay Portal 7.4.2 through 7.4.3.87, and Liferay DXP 7.4 before update 88 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a Vocabulary's 'description' text field.	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-42629	A-LIF-DIGI-241123/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-42629		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	5.4	Multiple stored cross-site scripting (XSS) vulnerabilities in the fragment components in Liferay Portal 7.4.2 through 7.4.3.53, and Liferay DXP 7.4 before update 54 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into any non-HTML field of a linked source asset. **CVE ID : CVE-2023-44309**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-44309	A-LIF-DIGI-241123/965
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	5.4	Stored cross-site scripting (XSS) vulnerability in Page Tree menu Liferay Portal 7.3.6 through 7.4.3.78, and Liferay DXP 7.3 fix pack 1 through update 23, and 7.4 before update 79 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into page's "Name" text field. **CVE ID : CVE-2023-44310**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-44310	A-LIF-DIGI-241123/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: liferay_portal					
Affected Version(s): From (including) 7.1.0 Up to (excluding) 7.4.3.88					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	5.4	Stored cross-site scripting (XSS) vulnerability in the Wiki widget in Liferay Portal 7.1.0 through 7.4.3.87, and Liferay DXP 7.0 fix pack 83 through 102, 7.1 fix pack 28 and earlier, 7.2 fix pack 20 and earlier, 7.3 update 33 and earlier, and 7.4 before update 88 allows remote attackers to inject arbitrary web script or HTML into a parent wiki page via a crafted payload injected into a wiki page's 'Content' text field. **CVE ID : CVE-2023-42628**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-42628	A-LIF-LIFE-241123/967
Affected Version(s): From (including) 7.3.5 Up to (excluding) 7.4.3.92					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	5.4	Multiple stored cross-site scripting (XSS) vulnerabilities in the Commerce module in Liferay Portal 7.3.5 through 7.4.3.91, and Liferay DXP 7.3 update 33 and earlier, and 7.4 before update 92 allow remote attackers to inject	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-42627	A-LIF-LIFE-241123/968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary web script or HTML via a crafted payload injected into a (1) Shipping Name, (2) Shipping Phone Number, (3) Shipping Address, (4) Shipping Address 2, (5) Shipping Address 3, (6) Shipping Zip, (7) Shipping City, (8) Shipping Region (9), Shipping Country, (10) Billing Name, (11) Billing Phone Number, (12) Billing Address, (13) Billing Address 2, (14) Billing Address 3, (15) Billing Zip, (16) Billing City, (17) Billing Region, (18) Billing Country, or (19) Region Code. **CVE ID : CVE-2023-42627**		
Affected Version(s): From (including) 7.3.6 Up to (excluding) 7.4.3.49					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	5.4	Stored cross-site scripting (XSS) vulnerability in Page Tree menu Liferay Portal 7.3.6 through 7.4.3.78, and Liferay DXP 7.3 fix pack 1 through update 23, and 7.4 before update 79 allows remote	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-44310	A-LIF-LIFE-241123/969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to inject arbitrary web script or HTML via a crafted payload injected into page's "Name" text field. **CVE ID : CVE-2023-44310**		
Affected Version(s): From (including) 7.4.2 Up to (excluding) 7.4.3.53					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	5.4	Multiple stored cross-site scripting (XSS) vulnerabilities in the fragment components in Liferay Portal 7.4.2 through 7.4.3.53, and Liferay DXP 7.4 before update 54 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into any non-HTML field of a linked source asset. **CVE ID : CVE-2023-44309**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-44309	A-LIF-LIFE-241123/970
Affected Version(s): From (including) 7.4.2 Up to (excluding) 7.4.3.88					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	5.4	Stored cross-site scripting (XSS) vulnerability in the manage vocabulary page in Liferay Portal 7.4.2 through 7.4.3.87, and Liferay DXP 7.4 before update 88 allows remote attackers to inject	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-42629	A-LIF-LIFE-241123/971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary web script or HTML via a crafted payload injected into a Vocabulary's 'description' text field. **CVE ID : CVE-2023-42629**		
Affected Version(s): From (including) 7.4.3.4 Up to (excluding) 7.4.3.86					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	6.1	Reflected cross-site scripting (XSS) vulnerability on the Export for Translation page in Liferay Portal 7.4.3.4 through 7.4.3.85, and Liferay DXP 7.4 before update 86 allows remote attackers to inject arbitrary web script or HTML via the `_com_liferay_translation_web_internal_portlet_TranslationPortlet_redirect` parameter. **CVE ID : CVE-2023-42497**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-42497	A-LIF-LIFE-241123/972
Affected Version(s): From (including) 7.4.3.41 Up to (excluding) 7.4.3.90					
Improper Neutralization of Input During Web Page Generation	17-Oct-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities in the Plugin for OAuth 2.0 module's OAuth2ProviderApplicationRedirect	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/	A-LIF-LIFE-241123/973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			class in Liferay Portal 7.4.3.41 through 7.4.3.89, and Liferay DXP 7.4 update 41 through update 89 allow remote attackers to inject arbitrary web script or HTML via the (1) code, or (2) error parameter. This issue is caused by an incomplete fix in CVE-2023-33941. **CVE ID : CVE-2023-44311**	cve-2023-44311	
Vendor: line					
Product: kaibutsunosato					
Affected Version(s): 13.6.1					
N/A	20-Oct-2023	5.3	The leakage of the client secret in Kaibutsunosato v13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages. **CVE ID : CVE-2023-39731**	https://liff.line.me/1657662489-pwEQNzJ4	A-LIN-KAIB-241123/974
Vendor: Linecorp					
Product: fukunaga_memberscard					
Affected Version(s): 13.6.1					
N/A	25-Oct-2023	8.2	The leakage of the client secret in Fukunaga_memberscard Line 13.6.1 allows attackers to obtain the channel access token and	N/A	A-LIN-FUKU-241123/975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			send crafted broadcast messages. **CVE ID : CVE-2023-39736**		
Product: line					
Affected Version(s): 13.6.1					
N/A	25-Oct-2023	7.5	An issue in Anglaise Company Anglaise.Company v.13.6.1 allows a remote attacker to obtain sensitive information via crafted GET request. **CVE ID : CVE-2023-38845**	N/A	A-LIN-LINE-241123/976
N/A	25-Oct-2023	7.5	An issue in Marbre Lapin Line v.13.6.1 allows a remote attacker to obtain sensitive information via crafted GET request. **CVE ID : CVE-2023-38846**	N/A	A-LIN-LINE-241123/977
N/A	25-Oct-2023	7.5	An issue in CHRISTINA JAPAN Line v.13.6.1 allows a remote attacker to obtain sensitive information via crafted GET request. **CVE ID : CVE-2023-38847**	N/A	A-LIN-LINE-241123/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Oct-2023	7.5	An issue in rmc R Beauty CLINIC Line v.13.6.1 allows a remote attacker to obtain sensitive information via crafted GET request. **CVE ID : CVE-2023-38848**	N/A	A-LIN-LINE-241123/979
N/A	25-Oct-2023	7.5	An issue in tire-sales Line v.13.6.1 allows a remote attacker to obtain sensitive information via crafted GET request. **CVE ID : CVE-2023-38849**	N/A	A-LIN-LINE-241123/980
Product: matsuya					
Affected Version(s): 13.6.1					
N/A	25-Oct-2023	8.2	The leakage of the client secret in Matsuya Line 13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages. **CVE ID : CVE-2023-39737**	N/A	A-LIN-MATS-241123/981
Product: onigiriya-musubee					
Affected Version(s): 13.6.1					
N/A	25-Oct-2023	8.2	The leakage of the client secret in Onigiriya-musubee Line 13.6.1 allows attackers to obtain the channel access	N/A	A-LIN-ONIG-241123/982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			token and send crafted broadcast messages. **CVE ID : CVE-2023-39740**		
Product: regina_sweets\&bakery					
Affected Version(s): 13.6.1					
N/A	25-Oct-2023	8.2	The leakage of the client secret in REGINA SWEETS&BAKERY Line 13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages. **CVE ID : CVE-2023-39739**	N/A	A-LIN-REGI-241123/983
Product: tokueimaru_waiting					
Affected Version(s): 13.6.1					
N/A	25-Oct-2023	8.2	The leakage of the client secret in Tokueimaru_waiting Line 13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages. **CVE ID : CVE-2023-39732**	N/A	A-LIN-TOKU-241123/984
Product: tonton-tei					
Affected Version(s): 13.6.1					
N/A	25-Oct-2023	8.2	The leakage of the client secret in TonTon-Tei Line v13.6.1 allows attackers to obtain	N/A	A-LIN-TONT-241123/985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the channel access token and send crafted broadcast messages. **CVE ID : CVE-2023-39733**		
Product: trackdiner10\/10_mc					
Affected Version(s): 13.6.1					
N/A	25-Oct-2023	8.2	The leakage of the client secret in VISION MEAT WORKS TrackDiner10/10_mc Line v13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages. **CVE ID : CVE-2023-39734**	https://liff.line.me/1660679145-eMKgg4rJ	A-LIN-TRAC-241123/986
Product: uomasa_saiji_new					
Affected Version(s): 13.6.1					
N/A	25-Oct-2023	8.2	The leakage of the client secret in Uomasa_Saiji_news Line 13.6.1 allows attackers to obtain the channel access token and send crafted broadcast messages. **CVE ID : CVE-2023-39735**	N/A	A-LIN-UOMA-241123/987
Vendor: linkstack					
Product: linkstack					
Affected Version(s): * Up to (excluding) 4.2.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weak Password Recovery Mechanism for Forgotten Password	29-Oct-2023	8.8	Weak Password Recovery Mechanism for Forgotten Password in GitHub repository linkstackorg/linkstack prior to v4.2.9. **CVE ID : CVE-2023-5840**	https://huntr.com/bounties/8042d8c3-650e-4c0d-9146-d9ccf6082b30, https://github.com/linkstackorg/linkstack/commit/fe7b99eae88f9e4c4cd4b00bab372cbf4b584b16	A-LIN-LINK-241123/988
Vendor: Linuxfoundation					
Product: nats-server					
Affected Version(s): From (including) 2.10.0 Up to (excluding) 2.10.2					
Incorrect Authorization	30-Oct-2023	6.5	NATS nats-server before 2.9.23 and 2.10.x before 2.10.2 has an authentication bypass. An implicit $G user in an authorization block can sometimes be used for unauthenticated access, even when the intention of the configuration was for each user to have an account. The earliest affected version is 2.2.0. **CVE ID : CVE-2023-47090**	https://github.com/nats-io/nats-server/security/advisories/GHSA-fr2g-9hjm-wr23	A-LIN-NATS-241123/989
Affected Version(s): From (including) 2.2.0 Up to (excluding) 2.9.23					
Incorrect Authorization	30-Oct-2023	6.5	NATS nats-server before 2.9.23 and 2.10.x before 2.10.2 has an authentication	https://github.com/nats-io/nats-server/security/advisories/GH	A-LIN-NATS-241123/990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass. An implicit $G user in an authorization block can sometimes be used for unauthenticated access, even when the intention of the configuration was for each user to have an account. The earliest affected version is 2.2.0. **CVE ID : CVE-2023-47090**	SA-fr2g-9hjm-wr23	
Vendor: lionscripts					
Product: webmaster_tools					
Affected Version(s): * Up to (including) 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in LionScripts.Com Webmaster Tools plugin <= 2.0 versions. **CVE ID : CVE-2023-46093**	N/A	A-LIO-WEBM-241123/991
Vendor: littlebigfresh					
Product: bunkum					
Affected Version(s): From (including) 4.0 Up to (excluding) 4.2.1					
Missing Release of Resource after Effective Lifetime	18-Oct-2023	5.3	Bunkum is an open-source protocol-agnostic request server for custom game servers. First, a little bit of background. So, in the beginning,	https://github.com/LittleBigRefresh/Bunkum/commit/6e109464ed9255f558182f001f475a378405ff76, https://github.com/LittleBigRef	A-LIT-BUNK-241123/992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bunkum's `AuthenticationService` only supported injecting `IUser`s. However, as Refresh and SoundShapesServer implemented permissions systems support for injecting `IToken`s into endpoints was added. All was well until 4.0. Bunkum 4.0 then changed to enforce relations between `IToken`s and `IUser`s. This wasn't implemented in a very good way in the `AuthenticationService`, and ended up breaking caching in such a way that cached tokens would persist after the lifetime of the request - since we tried to cache both tokens and users. From that point until now, from what I understand, Bunkum was attempting to use that cached token at the start of the next request once cached. Naturally, when that token expired,	resh/Bunkum/security/advisories/GHSA-jrf2-h5j6-3rrq	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			downstream projects like Refresh would remove the object from Realm - and cause the object in the cache to be in a detached state, causing an exception from invalid use of `IToken.User`. So in other words, a use-after-free since Realm can't manage the lifetime of the cached token. Security-wise, the scope is fairly limited, can only be pulled off on a couple endpoints given a few conditions, and you can't guarantee which token you're going to get. Also, the token *would* get invalidated properly if the endpoint had either a `IToken` usage or a `IUser` usage. The fix is to just wipe the token cache after the request was handled, which is now in `4.2.1`. Users are advised to upgrade. There are no known		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds for this vulnerability. **CVE ID : CVE-2023-45814**		
Vendor: longmenedutech					
Product: score_query_system					
Affected Version(s): 5.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	8.8	A vulnerability was found in Shaanxi Chanming Education Technology Score Query System 5.0. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument stuIdCard 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-243593 was assigned to this vulnerability. **CVE ID : CVE-2023-5787**	N/A	A-LON-SCOR-241123/993
Vendor: lylme					
Product: lylme_spage					
Affected Version(s): 1.7.0					
Improper Neutralization of Special	17-Oct-2023	9.8	lylme_spage v1.7.0 was discovered to contain a SQL injection	N/A	A-LYL-LYLM-241123/994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			vulnerability via the $userip parameter at function.php. **CVE ID : CVE-2023-45951**		
Unrestricted Upload of File with Dangerous Type	17-Oct-2023	9.8	An arbitrary file upload vulnerability in the component ajax_link.php of lylme_spage v1.7.0 allows attackers to execute arbitrary code via uploading a crafted file. **CVE ID : CVE-2023-45952**	N/A	A-LYL-LYLM-241123/995
Vendor: m-files					
Product: classic_web					
Affected Version(s): * Up to (excluding) 23.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	Stored XSS Vulnerability in M-Files Classic Web versions before 23.10 and LTS Service Release Versions before 23.2 LTS SR4 and 23.8 LTS SR1allows attacker to execute script on users browser via stored HTML document. **CVE ID : CVE-2023-2325**	https://www.m-files.com/about/trust-center/security-advisories/cve-2023-2325/	A-M-F-CLAS-241123/996
Affected Version(s): 23.2					
Improper Neutralization of Input	20-Oct-2023	5.4	Stored XSS Vulnerability in M-Files Classic Web versions before	https://www.m-files.com/about/trust-	A-M-F-CLAS-241123/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			23.10 and LTS Service Release Versions before 23.2 LTS SR4 and 23.8 LTS SR1allows attacker to execute script on users browser via stored HTML document. **CVE ID : CVE-2023-2325**	center/security-advisories/cve-2023-2325/	
Affected Version(s): 23.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	Stored XSS Vulnerability in M-Files Classic Web versions before 23.10 and LTS Service Release Versions before 23.2 LTS SR4 and 23.8 LTS SR1allows attacker to execute script on users browser via stored HTML document. **CVE ID : CVE-2023-2325**	https://www.m-files.com/about/trust-center/security-advisories/cve-2023-2325/	A-M-F-CLAS-241123/998
Product: web_companion					
Affected Version(s): 23.8					
Inclusion of Functionality from Untrusted Control Sphere	20-Oct-2023	7.8	Execution of downloaded content flaw in M-Files Web Companion before release version 23.10 and LTS Service Release Versions before 23.8 LTS SR1 allows	https://www.m-files.com/about/trust-center/security-advisories/cve-2023-5523/	A-M-F-WEB_-241123/999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution **CVE ID : CVE-2023-5523**		
Unrestricted Upload of File with Dangerous Type	20-Oct-2023	7.3	Insufficient blacklisting in M-Files Web Companion before release version 23.10 and LTS Service Release Versions before 23.8 LTS SR1 allows Remote Code Execution via specific file types **CVE ID : CVE-2023-5524**	https://www.m-files.com/about/trust-center/security-advisories/cve-2023-5524/	A-M-F-WEB_-241123/1000
Affected Version(s): * Up to (excluding) 23.8					
Inclusion of Functionality from Untrusted Control Sphere	20-Oct-2023	7.8	Execution of downloaded content flaw in M-Files Web Companion before release version 23.10 and LTS Service Release Versions before 23.8 LTS SR1 allows Remote Code Execution **CVE ID : CVE-2023-5523**	https://www.m-files.com/about/trust-center/security-advisories/cve-2023-5523/	A-M-F-WEB_-241123/1001
Unrestricted Upload of File with	20-Oct-2023	7.3	Insufficient blacklisting in M-Files Web	https://www.m-files.com/about	A-M-F-WEB_-241123/1002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			Companion before release version 23.10 and LTS Service Release Versions before 23.8 LTS SR1 allows Remote Code Execution via specific file types **CVE ID : CVE-2023-5524**	/trust-center/security-advisories/cve-2023-5524/	
Affected Version(s): From (including) 23.3 Up to (excluding) 23.10					
Inclusion of Functionality from Untrusted Control Sphere	20-Oct-2023	7.8	Execution of downloaded content flaw in M-Files Web Companion before release version 23.10 and LTS Service Release Versions before 23.8 LTS SR1 allows Remote Code Execution **CVE ID : CVE-2023-5523**	https://www.m-files.com/about/trust-center/security-advisories/cve-2023-5523/	A-M-F-WEB_-241123/1003
Unrestricted Upload of File with Dangerous Type	20-Oct-2023	7.3	Insufficient blacklisting in M-Files Web Companion before release version 23.10 and LTS Service Release Versions before 23.8 LTS SR1 allows	https://www.m-files.com/about/trust-center/security-advisories/cve-2023-5524/	A-M-F-WEB_-241123/1004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution via specific file types **CVE ID : CVE-2023-5524**		
Vendor: macwk					
Product: icecms					
Affected Version(s): 2.0.1					
Cross-Site Request Forgery (CSRF)	27-Oct-2023	6.5	IceCMS v2.0.1 is vulnerable to Cross Site Request Forgery (CSRF). **CVE ID : CVE-2023-42188**	https://github.com/Thecosy/IceCMS/issues/17	A-MAC-ICEC-241123/1005
Vendor: madfishdigital					
Product: bulk_noindex_\&_nofollow_toolkit					
Affected Version(s): * Up to (excluding) 1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Mad Fish Digital Bulk NoIndex & NoFollow Toolkit plugin <= 1.42 versions. **CVE ID : CVE-2023-45065**	N/A	A-MAD-BULK-241123/1006
Vendor: maheshwaghmare					
Product: copy_anything_to_clipboard					
Affected Version(s): * Up to (excluding) 2.6.5					
Improper Neutralization of Input During Web Page Generation	20-Oct-2023	5.4	The Copy Anything to Clipboard plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'copy' shortcode in	https://plugins.trac.wordpress.org/changeset/2969441/copy-the-code#file1, https://www.wordfence.com/t	A-MAH-COPY-241123/1007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			versions up to, and including, 2.6.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5086**	hreat-intel/vulnerabilities/id/e834a211-ccc8-4a30-a15d-879ba34184e9?source=cve	
Vendor: mahlamusa					
Product: who_hit_the_page_hit_counter					
Affected Version(s): * Up to (including) 1.4.14.3					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Mahlamusa Who Hit The Page – Hit Counter plugin <= 1.4.14.3 versions. **CVE ID : CVE-2023-46087**	N/A	A-MAH-WHO_-241123/1008
Vendor: maileon					
Product: maileon					
Affected Version(s): * Up to (excluding) 2.16.1					
Improper Neutralization of	25-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS)	N/A	A-MAI-MAIL-241123/1009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			vulnerability in XQueue GmbH Maileon for WordPress plugin <= 2.16.0 versions. **CVE ID : CVE-2023-46068**		
Vendor: mailmunch					
Product: constant_contact_forms					
Affected Version(s): * Up to (including) 2.0.10					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in MailMunch Constant Contact Forms by MailMunch plugin <= 2.0.10 versions. **CVE ID : CVE-2023-45647**	N/A	A-MAI-CONS-241123/1010
Product: mailchimp_forms					
Affected Version(s): * Up to (including) 3.1.4					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in MailMunch MailChimp Forms by MailMunch plugin <= 3.1.4 versions. **CVE ID : CVE-2023-45748**	N/A	A-MAI-MAIL-241123/1011
Vendor: man					
Product: d-tale					
Affected Version(s): * Up to (excluding) 3.7.0					
N/A	25-Oct-2023	9.8	D-Tale is the combination of a Flask back-end and a React front-end	https://github.com/man-group/dtale/security/advisorie	A-MAN-D-TA-241123/1012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to view & analyze Pandas data structures. Prior to version 3.7.0, users hosting D-Tale publicly can be vulnerable to remote code execution, allowing attackers to run malicious code on the server. This issue has been patched in version 3.7.0 by turning off "Custom Filter" input by default. The only workaround for versions earlier than 3.7.0 is to only host D-Tale to trusted users. **CVE ID : CVE-2023-46134**	s/GHSA-jq6c-r9xf-qxjm, https://github.com/man-group/dtale/commit/bf8c54ab2490803f45f0652a9a0e221a94d39668	
Vendor: Mantisbt					
Product: mantisbt					
Affected Version(s): * Up to (excluding) 2.25.8					
Exposure of Resource to Wrong Sphere	16-Oct-2023	4.3	MantisBT is an open source bug tracker. Due to insufficient access-level checks on the Wiki redirection page, any user can reveal private Projects' names, by accessing wiki.php with sequentially incremented IDs. This issue has been	https://github.com/mantisbt/mantisbt/commit/65c44883f9d24f3ccef066fb523c93d8fdd7afc1, https://github.com/mantisbt/mantisbt/security/advisories/GHSA-v642-mh27-8j6m,	A-MAN-MANT-241123/1013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addressed in commit `65c44883f` which has been included in release `2.258`. Users are advised to upgrade. Users unable to upgrade should disable wiki integration (`$g_wiki_enable = OFF;`). **CVE ID : CVE-2023-44394**	https://mantisbt.org/bugs/view.php?id=32981	
Vendor: marcomilesi					
Product: wp_attachments					
Affected Version(s): * Up to (including) 5.0.6					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Marco Milesi WP Attachments plugin <= 5.0.6 versions. **CVE ID : CVE-2023-45651**	N/A	A-MAR-WP_A-241123/1014
Vendor: martmbithi					
Product: internet_banking_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Oct-2023	6.1	A vulnerability was found in CodeAstro Internet Banking System 1.0. It has been classified as problematic. Affected is an unknown function of the file pages_system_settings.php. The manipulation of the argument	N/A	A-MAR-INTE-241123/1015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sys_name with the input <ScRiPt >alert(991)</ScRi Pt> 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-243132. **CVE ID : CVE-2023-5694**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Oct-2023	6.1	A vulnerability was found in CodeAstro Internet Banking System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file pages_reset_pwd.php. The manipulation of the argument email with the input testing%40example.com'%26%25<ScRiPt%20>alert(9860)</ScRiPt> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may	N/A	A-MAR-INTE-241123/1016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. The identifier VDB-243133 was assigned to this vulnerability. **CVE ID : CVE-2023-5695**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Oct-2023	6.1	A vulnerability was found in CodeAstro Internet Banking System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file pages_transfer_money.php. The manipulation of the argument account_number with the input 357146928--><ScRiPt%20>alert(9206)</ScRiPt><!-- leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-243134 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-5696**	N/A	A-MAR-INTE-241123/1017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	6.1	A vulnerability classified as problematic has been found in CodeAstro Internet Banking System 1.0. This affects an unknown part of the file pages_withdraw_money.php. The manipulation of the argument account_number with the input 287359614--><ScRiPt%20>alert(1234)</ScRiPt><!-- leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-243135. **CVE ID : CVE-2023-5697**	N/A	A-MAR-INTE-241123/1018
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	6.1	A vulnerability classified as problematic was found in CodeAstro Internet Banking System 1.0. This vulnerability affects unknown code of the file pages_deposit_mon	N/A	A-MAR-INTE-241123/1019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ey.php. The manipulation of the argument account_number with the input 421873905--><ScRiPt%20>alert(9523)</ScRiPt><!-- leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-243136. **CVE ID : CVE-2023-5698**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	6.1	A vulnerability, which was classified as problematic, has been found in CodeAstro Internet Banking System 1.0. This issue affects some unknown processing of the file pages_view_client.php. The manipulation of the argument acc_name with the input Johnnie Reyes'"()&%<zzz><ScRiPt >alert(5646)</ScRiPt> leads to cross	N/A	A-MAR-INTE-241123/1020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-243137 was assigned to this vulnerability. **CVE ID : CVE-2023-5699**		
Product: pos_system					
Affected Version(s): 1					
Unrestricted Upload of File with Dangerous Type	26-Oct-2023	8.8	A vulnerability was found in CodeAstro POS System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /profil of the component Profile Picture Handler. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-243601 was assigned to this vulnerability. **CVE ID : CVE-2023-5795**	N/A	A-MAR-POS_-241123/1021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	26-Oct-2023	8.8	A vulnerability was found in CodeAstro POS System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /setting of the component Logo Handler. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-243602 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-5796**	N/A	A-MAR-POS_-241123/1022
Vendor: matter-labs					
Product: zkvyper					
Affected Version(s): * Up to (excluding) 1.3.10					
N/A	25-Oct-2023	5.3	era-compiler-vyper is the EraVM Vyper compiler for zkSync Era, a layer 2 rollup that uses zero-knowledge proofs to scale Ethereum. Prior to era-compiler-vype version 1.3.10, a bug prevented the initialization of the first immutable variable for Vyper	https://github.com/matter-labs/era-compiler-vyper/commit/8be305a1b9c68d0fd47dad3434224ed85944ca25, https://github.com/matter-labs/era-compiler-vyper/security/	A-MAT-ZKVY-241123/1023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contracts meeting certain criteria. The problem arises when there is a String or Array with more 256-bit words allocated than initialized. It results in the second word's index unset, that is effectively set to 0, so the first immutable value with the actual 0 index is overwritten in the ImmutableSimulator. Version 1.3.10 fixes this issue by setting all indexes in advance. The problem will go away, but it will get more expensive if the user allocates a lot of uninitialized space, e.g. `String[4096]`. Upgrading and redeploying affected contracts is the only way of working around the issue. **CVE ID : CVE-2023-46232**	advisories/GHSA-h8jv-969m-94r4	
Vendor: mattermost					
Product: mattermost					
Affected Version(s): * Up to (excluding) 2.8.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Oct-2023	4.3	Mattermost Mobile fails to limit the maximum number of Markdown elements in a post allowing an attacker to send a post with hundreds of emojis to a channel and freeze the mobile app of users when viewing that particular channel. **CVE ID : CVE-2023-5522**	https://mattermost.com/security-updates	A-MAT-MATT-241123/1024
Product: mattermost_desktop					
Affected Version(s): * Up to (including) 5.4.0					
Insertion of Sensitive Information into Log File	17-Oct-2023	5.5	Mattermost Desktop fails to set an appropriate log level during initial run after fresh installation resulting in logging all keystrokes including password entry being logged. **CVE ID : CVE-2023-5339**	https://mattermost.com/security-updates	A-MAT-MATT-241123/1025
Vendor: matthewschwartz					
Product: google_maps_made_simple					
Affected Version(s): * Up to (including) 0.6					
Improper Neutralization of Special Elements used in an SQL Command	30-Oct-2023	8.8	The Google Maps made Simple plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to,	https://plugins.trac.wordpress.org/browser/wp-gmappity-easy-google-maps/tags/0.6/wpgmappity-	A-MAT-GOOG-241123/1026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			and including, 0.6 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-5315**	metadata.php#L127	
Vendor: mattmckenny					
Product: stout_google_calendar					
Affected Version(s): * Up to (including) 1.2.3					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Matt McKenny Stout Google Calendar plugin <= 1.2.3 versions. **CVE ID : CVE-2023-45273**	N/A	A-MAT-STOU-241123/1027
Vendor: maurice					
Product: vrm360					
Affected Version(s): * Up to (including) 1.2.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Oct-2023	5.3	The Vrm 360 3D Model Viewer WordPress plugin through 1.2.1 exposes the full path of a file when putting in a non-existent file in a parameter of the shortcode. **CVE ID : CVE-2023-5177**	N/A	A-MAU-VRM3-241123/1028
Vendor: mayurik					
Product: best_courier_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Oct-2023	9.8	Sourcecodester Best Courier Management System 1.0 is vulnerable to SQL Injection via the parameter id in /edit_branch.php. **CVE ID : CVE-2023-46005**	N/A	A-MAY-BEST-241123/1029
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Oct-2023	9.8	Sourcecodester Best Courier Management System 1.0 is vulnerable to SQL Injection via the parameter id in /edit_user.php. **CVE ID : CVE-2023-46006**	N/A	A-MAY-BEST-241123/1030
Improper Neutralization of Special Elements used in an	18-Oct-2023	9.8	Sourcecodester Best Courier Management System 1.0 is vulnerable to SQL Injection via the	N/A	A-MAY-BEST-241123/1031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			parameter id in /edit_staff.php. **CVE ID : CVE-2023-46007**		
Unrestricted Upload of File with Dangerous Type	18-Oct-2023	7.2	Sourcecodester Best Courier Management System 1.0 is vulnerable to Arbitrary file upload in the update_user function. **CVE ID : CVE-2023-46004**	N/A	A-MAY-BEST-241123/1032
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Oct-2023	5.4	Best Courier Management System v1.0 is vulnerable to Cross Site Scripting (XSS) in the change username field. **CVE ID : CVE-2023-46451**	N/A	A-MAY-BEST-241123/1033
Product: inventory_management_system					
Affected Version(s): 1.0					
Incorrect Permission Assignment for Critical Resource	26-Oct-2023	8.8	Sourcecodester Free and Open Source inventory management system v1.0 is vulnerable to Incorrect Access Control. An arbitrary user can change the password of another user and takeover the account via IDOR in	N/A	A-MAY-INVE-241123/1034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the password change function. **CVE ID : CVE-2023-46449**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2023	5.4	Sourcecodester Free and Open Source inventory management system 1.0 is vulnerable to Cross Site Scripting (XSS) via the Add supplier function. **CVE ID : CVE-2023-46450**	N/A	A-MAY-INVE-241123/1035
Vendor: mbconnectline					
Product: mbconnect24					
Affected Version(s): * Up to (including) 2.14.2					
Improper Privilege Management	16-Oct-2023	4.3	In Red Lion Europe mbCONNECT24 and mymbCONNECT24 and Helmholz myREX24 and myREX24.virtual up to and including 2.14.2 an improperly implemented access validation allows an authenticated, low privileged attacker to gain read access to limited, non-critical device information in his account he should not have access to. **CVE ID : CVE-2023-4834**	N/A	A-MBC-MBCO-241123/1036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mymbconnect24					
Affected Version(s): * Up to (including) 2.14.2					
Improper Privilege Management	16-Oct-2023	4.3	In Red Lion Europe mbCONNECT24 and mymbCONNECT24 and Helmholz myREX24 and myREX24.virtual up to and including 2.14.2 an improperly implemented access validation allows an authenticated, low privileged attacker to gain read access to limited, non-critical device information in his account he should not have access to. **CVE ID : CVE-2023-4834**	N/A	A-MBC-MYMB-241123/1037
Vendor: Memcached					
Product: memcached					
Affected Version(s): * Up to (excluding) 1.6.22					
Off-by-one Error	27-Oct-2023	9.8	In Memcached before 1.6.22, an off-by-one error exists when processing proxy requests in proxy mode, if \n is used instead of \r\n. **CVE ID : CVE-2023-46853**	https://github.com/memcached/memcached/commit/6987918e9a3094ec4fc8976f01f769f624d790fa	A-MEM-MEMC-241123/1038
Buffer Copy without	27-Oct-2023	7.5	In Memcached before 1.6.22, a buffer overflow	https://github.com/memcached/memcached/c	A-MEM-MEMC-241123/1039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			exists when processing multiget requests in proxy mode, if there are many spaces after the "get" substring. **CVE ID : CVE-2023-46852**	ommit/76a6c363c18cfe7b6a1524ae64202ac9db330767	
Vendor: metagauss					
Product: eventprime					
Affected Version(s): * Up to (including) 3.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in EventPrime EventPrime – Events Calendar, Bookings and Tickets plugin <= 3.1.5 versions. **CVE ID : CVE-2023-45637**	N/A	A-MET-EVEN-241123/1040
Vendor: michaeluno					
Product: auto_amazon_links					
Affected Version(s): * Up to (excluding) 5.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	The Auto Amazon Links plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the style parameter in versions up to, and including, 5.3.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2961861%40amazon-auto-links%2Ftrunk&old=2896127%40amazon-auto-links%2Ftrunk	A-MIC-AUTO-241123/1041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers with contributor access to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-4482**	&sfp_email=&sfph_mail=	
Vendor: Microfocus					
Product: asset_management_x					
Affected Version(s): 2021.08					
URL Redirection to Untrusted Site ('Open Redirect')	30-Oct-2023	6.1	Potential open redirect vulnerability in opentext Service Management Automation X (SMAX) versions 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11 and opentext Asset Management X (AMX) versions 2021.08, 2021.11, 2022.05, 2022.11. The vulnerability could allow attackers to redirect a user to malicious websites. **CVE ID : CVE-2023-4964**	https://portal.microfocus.com/s/article/KM000022703?language=en_US	A-MIC-ASSE-241123/1042
Affected Version(s): 2021.11					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	30-Oct-2023	6.1	Potential open redirect vulnerability in opentext Service Management Automation X (SMAX) versions 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11 and opentext Asset Management X (AMX) versions 2021.08, 2021.11, 2022.05, 2022.11. The vulnerability could allow attackers to redirect a user to malicious websites. **CVE ID : CVE-2023-4964**	https://portal.microfocus.com/s/article/KM000022703?language=en_US	A-MIC-ASSE-241123/1043
Affected Version(s): 2022.05					
URL Redirection to Untrusted Site ('Open Redirect')	30-Oct-2023	6.1	Potential open redirect vulnerability in opentext Service Management Automation X (SMAX) versions 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11 and opentext Asset	https://portal.microfocus.com/s/article/KM000022703?language=en_US	A-MIC-ASSE-241123/1044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management X (AMX) versions 2021.08, 2021.11, 2022.05, 2022.11. The vulnerability could allow attackers to redirect a user to malicious websites. **CVE ID : CVE-2023-4964**		
Affected Version(s): 2022.11					
URL Redirection to Untrusted Site ('Open Redirect')	30-Oct-2023	6.1	Potential open redirect vulnerability in opentext Service Management Automation X (SMAX) versions 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11 and opentext Asset Management X (AMX) versions 2021.08, 2021.11, 2022.05, 2022.11. The vulnerability could allow attackers to redirect a user to malicious websites. **CVE ID : CVE-2023-4964**	https://portal.microfocus.com/s/article/KM000022703?language=en_US	A-MIC-ASSE-241123/1045
Product: service_management_automation_x					
Affected Version(s): 2021.08					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	30-Oct-2023	6.1	Potential open redirect vulnerability in opentext Service Management Automation X (SMAX) versions 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11 and opentext Asset Management X (AMX) versions 2021.08, 2021.11, 2022.05, 2022.11. The vulnerability could allow attackers to redirect a user to malicious websites. **CVE ID : CVE-2023-4964**	https://portal.microfocus.com/s/article/KM000022703?language=en_US	A-MIC-SERV-241123/1046
Affected Version(s): 2021.11					
URL Redirection to Untrusted Site ('Open Redirect')	30-Oct-2023	6.1	Potential open redirect vulnerability in opentext Service Management Automation X (SMAX) versions 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11 and opentext Asset Management X (AMX) versions	https://portal.microfocus.com/s/article/KM000022703?language=en_US	A-MIC-SERV-241123/1047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2021.08, 2021.11, 2022.05, 2022.11. The vulnerability could allow attackers to redirect a user to malicious websites. **CVE ID : CVE-2023-4964**		
Affected Version(s): 2022.05					
URL Redirection to Untrusted Site ('Open Redirect')	30-Oct-2023	6.1	Potential open redirect vulnerability in opentext Service Management Automation X (SMAX) versions 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11 and opentext Asset Management X (AMX) versions 2021.08, 2021.11, 2022.05, 2022.11. The vulnerability could allow attackers to redirect a user to malicious websites. **CVE ID : CVE-2023-4964**	https://portal.microfocus.com/s/article/KM000022703?language=en_US	A-MIC-SERV-241123/1048
Affected Version(s): 2022.11					
URL Redirection to Untrusted	30-Oct-2023	6.1	Potential open redirect vulnerability	https://portal.microfocus.com/s/article/KM0	A-MIC-SERV-241123/1049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Site ('Open Redirect')			in opentext Service Management Automation X (SMAX) versions 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11 and opentext Asset Management X (AMX) versions 2021.08, 2021.11, 2022.05, 2022.11. The vulnerability could allow attackers to redirect a user to malicious websites. **CVE ID : CVE-2023-4964**	00022703?language=en_US	
Affected Version(s): 2020.05					
URL Redirection to Untrusted Site ('Open Redirect')	30-Oct-2023	6.1	Potential open redirect vulnerability in opentext Service Management Automation X (SMAX) versions 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11 and opentext Asset Management X (AMX) versions 2021.08, 2021.11, 2022.05, 2022.11. The	https://portal.microfocus.com/s/article/KM000022703?language=en_US	A-MIC-SERV-241123/1050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability could allow attackers to redirect a user to malicious websites. **CVE ID : CVE-2023-4964**		
Affected Version(s): 2020.08					
URL Redirection to Untrusted Site ('Open Redirect')	30-Oct-2023	6.1	Potential open redirect vulnerability in opentext Service Management Automation X (SMAX) versions 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11 and opentext Asset Management X (AMX) versions 2021.08, 2021.11, 2022.05, 2022.11. The vulnerability could allow attackers to redirect a user to malicious websites. **CVE ID : CVE-2023-4964**	https://portal.microfocus.com/s/article/KM000022703?language=en_US	A-MIC-SERV-241123/1051
Affected Version(s): 2020.11					
URL Redirection to Untrusted Site ('Open Redirect')	30-Oct-2023	6.1	Potential open redirect vulnerability in opentext Service Management Automation X	https://portal.microfocus.com/s/article/KM000022703?language=en_US	A-MIC-SERV-241123/1052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SMAX) versions 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11 and opentext Asset Management X (AMX) versions 2021.08, 2021.11, 2022.05, 2022.11. The vulnerability could allow attackers to redirect a user to malicious websites. **CVE ID : CVE-2023-4964**		
Affected Version(s): 2021.02					
URL Redirection to Untrusted Site ('Open Redirect')	30-Oct-2023	6.1	Potential open redirect vulnerability in opentext Service Management Automation X (SMAX) versions 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11 and opentext Asset Management X (AMX) versions 2021.08, 2021.11, 2022.05, 2022.11. The vulnerability could allow attackers to redirect a user to	https://portal.microfocus.com/s/article/KM000022703?language=en_US	A-MIC-SERV-241123/1053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious websites. **CVE ID : CVE-2023-4964**		
Affected Version(s): 2021.05					
URL Redirection to Untrusted Site ('Open Redirect')	30-Oct-2023	6.1	Potential open redirect vulnerability in opentext Service Management Automation X (SMAX) versions 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11 and opentext Asset Management X (AMX) versions 2021.08, 2021.11, 2022.05, 2022.11. The vulnerability could allow attackers to redirect a user to malicious websites. **CVE ID : CVE-2023-4964**	https://portal.microfocus.com/s/article/KM000022703?language=en_US	A-MIC-SERV-241123/1054
Vendor: Microsoft					
Product: edge_chromium					
Affected Version(s): * Up to (excluding) 118.0.2088.76					
Use After Free	30-Oct-2023	5.5	Adobe Acrobat for Edge version 118.0.2088.46 (and earlier) is affected by a Use After Free vulnerability. An unauthenticated attacker could	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-44323	A-MIC-EDGE-241123/1055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44323**		
Vendor: Microweber					
Product: microweber					
Affected Version(s): * Up to (excluding) 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Oct-2023	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 2.0. **CVE ID : CVE-2023-5861**	https://github.com/microweber/microweber/commit/6ed7ebf1631dd8f0780caa4151a5538f3b227d26, https://huntr.com/bounties/7baecef8-6c59-42fc-bced-886c4929e220	A-MIC-MICR-241123/1056
Vendor: minical					
Product: minical					
Affected Version(s): 1.0.0					
Authorization Bypass Through User-Controlled Key	30-Oct-2023	8.8	An issue in minCal v.1.0.0 allows a remote attacker to execute arbitrary code via a crafted script to the customer_data parameter.	N/A	A-MIN-MINI-241123/1057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46478		
Vendor: miniorange					
Product: active_directory_integration_\/_ldap_integration					
Affected Version(s): * Up to (excluding) 4.1.10					
N/A	16-Oct-2023	7.5	The Active Directory Integration / LDAP Integration WordPress plugin before 4.1.10 stores sensitive LDAP logs in a buffer file when an administrator wants to export said logs. Unfortunately, this log file is never removed, and remains accessible to any users knowing the URL to do so. **CVE ID : CVE-2023-5003**	N/A	A-MIN-ACTI-241123/1058
Vendor: mintty_project					
Product: mintty					
Affected Version(s): * Up to (including) 3.6.4					
N/A	26-Oct-2023	9.8	An issue in Mintty v.3.6.4 and before allows a remote attacker to execute arbitrary code via crafted commands to the terminal. **CVE ID : CVE-2023-39726**	N/A	A-MIN-MINT-241123/1059
Vendor: mlsoft					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: tco\!stream					
Affected Version(s): * Up to (excluding) 8.0.23.215					
Download of Code Without Integrity Check	30-Oct-2023	9.8	In MLSoft TCO!stream versions 8.0.22.1115 and below, a vulnerability exists due to insufficient permission validation. This allows an attacker to make the victim download and execute arbitrary files. **CVE ID : CVE-2023-45799**	N/A	A-MLS-TCO\-241123/1060
Vendor: mnbvcxz131421					
Product: douhaocms					
Affected Version(s): 3.3					
Cross-Site Request Forgery (CSRF)	30-Oct-2023	8.8	Cross Site Request Forgery (CSRF) vulnerability in DouHaocms v.3.3 allows a remote attacker to execute arbitrary code via the adminAction.class.php file. **CVE ID : CVE-2023-42323**	N/A	A-MNB-DOUH-241123/1061
Vendor: modoboa					
Product: modoboa					
Affected Version(s): * Up to (excluding) 2.2.2					
Cross-Site Request	20-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) in GitHub repository	https://huntr.com/bounties/980c75a5-d978-4b0e-9bcc-	A-MOD-MODO-241123/1062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			modoboa/modoboa prior to 2.2.2. **CVE ID : CVE-2023-5690**	2b2682c97e01, https://github.com/modoboa/modoboa/commit/23e4c25511c66c0548da001236f47e19e3f9e4d9	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	Cross-site Scripting (XSS) - DOM in GitHub repository modoboa/modoboa prior to 2.2.2. **CVE ID : CVE-2023-5688**	https://huntr.com/bounties/0ceb10e4-952b-4ca4-baf8-5b6f12e3a8a7, https://github.com/modoboa/modoboa/commit/d33d3cd2d11dbfebd8162c46e2c2a9873919a967	A-MOD-MODO-241123/1063
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	Cross-site Scripting (XSS) - DOM in GitHub repository modoboa/modoboa prior to 2.2.2. **CVE ID : CVE-2023-5689**	https://github.com/modoboa/modoboa/commit/d33d3cd2d11dbfebd8162c46e2c2a9873919a967, https://huntr.com/bounties/24835833-3421-412b-bafb-1b7ea3cf60e6	A-MOD-MODO-241123/1064
Vendor: monospace					
Product: directus					
Affected Version(s): From (including) 10.4.0 Up to (excluding) 10.6.2					
Improper Handling of Exceptional Conditions	19-Oct-2023	6.5	Directus is a real-time API and App dashboard for managing SQL database content. In affected versions any Directus	https://github.com/directus/directus/security/advisories/GHSA-hmgw-9jrg-hf2m, https://github.c	A-MON-DIRE-241123/1065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			installation that has websockets enabled can be crashed if the websocket server receives an invalid frame. A malicious user could leverage this bug to crash Directus. This issue has been addressed in version 10.6.2. Users are advised to upgrade. Users unable to upgrade should avoid using websockets. **CVE ID : CVE-2023-45820**	om/directus/directus/commit/243eed781b42d6b4948ddb8c3792bcf5b44f55bb	
Vendor: monsterinsights					
Product: user_feedback					
Affected Version(s): * Up to (including) 1.0.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	6.1	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in UserFeedback Team User Feedback plugin <= 1.0.9 versions. **CVE ID : CVE-2023-46153**	N/A	A-MON-USER-241123/1066
Vendor: Moodle					
Product: moodle					
Affected Version(s): 4.3.0					
Improper Neutralization of Input During Web Page	29-Oct-2023	5.4	Moodle 4.3 allows /grade/report/grader/index.php?searchvalue= reflected XSS when logged in as a teacher. NOTE:	N/A	A-MOO-MOOD-241123/1067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			the Moodle Security FAQ link states "Some forms of rich content [are] used by teachers to enhance their courses ... admins and teachers can post XSS-capable content, but students can not." **CVE ID : CVE-2023-46858**		
Vendor: moosocial					
Product: moosocial					
Affected Version(s): 3.1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-2023	6.1	Cross Site Scripting vulnerability in mooSocial 3.1.8 allows a remote attacker to obtain sensitive information via a crafted script to the q parameter in the Search function. **CVE ID : CVE-2023-45542**	N/A	A-MOO-MOOS-241123/1068
Vendor: mosparo					
Product: mosparo					
Affected Version(s): * Up to (excluding) 1.0.3					
Cross-Site Request Forgery (CSRF)	20-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) in GitHub repository mosparo/mosparo prior to 1.0.3. **CVE ID : CVE-2023-5687**	https://huntr.com/bounties/33f95510-cdee-460e-8e61-107874962f2d, https://github.com/mosparo/mosparo/commit/fb3ac528b754	A-MOS-MOSP-241123/1069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				8beb802182310967968a21c1354a	
Vendor: Mozilla					
Product: firefox					
Affected Version(s): * Up to (excluding) 117.0					
N/A	25-Oct-2023	6.5	An attacker could have created a malicious link using bidirectional characters to spoof the location in the address bar when visited. This vulnerability affects Firefox < 117, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5732**	https://www.mozilla.org/security/advisories/mfsa2023-34/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1690979	A-MOZ-FIRE-241123/1070
Affected Version(s): * Up to (excluding) 119.0					
Out-of-bounds Write	25-Oct-2023	9.8	Memory safety bugs present in Firefox 118, Firefox ESR 115.3, and Thunderbird 115.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/	A-MOZ-FIRE-241123/1071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 115.4.1. **CVE ID : CVE-2023-5730**		
Out-of-bounds Write	25-Oct-2023	9.8	Memory safety bugs present in Firefox 118. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 119. **CVE ID : CVE-2023-5731**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://bugzilla.mozilla.org/buglist.cgi?bug_id=1690111%2C1721904%2C1851803%2C1854068	A-MOZ-FIRE-241123/1072
N/A	25-Oct-2023	7.5	Drivers are not always robust to extremely large draw calls and in some cases this scenario could have led to a crash. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5724**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1836705	A-MOZ-FIRE-241123/1073
N/A	25-Oct-2023	7.5	During garbage collection extra operations were performed on a object that should	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.m	A-MOZ-FIRE-241123/1074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not be. This could have led to a potentially exploitable crash. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5728**	ozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1852729	
N/A	25-Oct-2023	6.5	The executable file warning was not presented when downloading .msix, .msixbundle, .appx, and .appxbundle files, which can run commands on a user's computer. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.* This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5727**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1847180	A-MOZ-FIRE-241123/1075
Improper Neutralization of Input During Web Page	25-Oct-2023	6.1	When opening a page in reader mode, the redirect URL could have caused attacker-controlled script to	https://www.mozilla.org/security/advisories/mfsa2023-48/	A-MOZ-FIRE-241123/1076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			execute in a reflected Cross-Site Scripting (XSS) attack. This vulnerability affects Firefox for iOS < 119. **CVE ID : CVE-2023-5758**		
Observable Discrepancy	25-Oct-2023	5.3	Using iterative requests an attacker was able to learn the size of an opaque response, as well as the contents of a server-supplied Vary header. This vulnerability affects Firefox < 119. **CVE ID : CVE-2023-5722**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://bugzilla.mozilla.org/show_bug.cgi?id=1738426	A-MOZ-FIRE-241123/1077
N/A	25-Oct-2023	5.3	An attacker with temporary script access to a site could have set a cookie containing invalid characters using `document.cookie` that could have led to unknown errors. This vulnerability affects Firefox < 119. **CVE ID : CVE-2023-5723**	https://www.mozilla.org/security/advisories/mfsa2023-45/	A-MOZ-FIRE-241123/1078
Improper Restriction of Rendered	25-Oct-2023	4.3	It was possible for certain browser prompts and dialogs to be	https://www.mozilla.org/security/advisories/mfsa2023-45/,	A-MOZ-FIRE-241123/1079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
UI Layers or Frames			activated or dismissed unintentionally by the user due to an insufficient activation-delay. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5721**	https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1830820	
N/A	25-Oct-2023	4.3	A malicious installed WebExtension could open arbitrary URLs, which under the right circumstance could be leveraged to collect sensitive user data. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5725**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://bugzilla.mozilla.org/show_bug.cgi?id=1845739, https://www.mozilla.org/security/advisories/mfsa2023-46/	A-MOZ-FIRE-241123/1080
N/A	25-Oct-2023	4.3	A website could have obscured the full screen notification by using the file open dialog. This could have led to user confusion and possible spoofing attacks.	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/	A-MOZ-FIRE-241123/1081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: This issue only affected macOS operating systems. Other operating systems are unaffected. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5726**	mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1846205	
N/A	25-Oct-2023	4.3	A malicious web site can enter fullscreen mode while simultaneously triggering a WebAuthn prompt. This could have obscured the fullscreen notification and could have been leveraged in a spoofing attack. This vulnerability affects Firefox < 119. **CVE ID : CVE-2023-5729**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://bugzilla.mozilla.org/show_bug.cgi?id=1823720	A-MOZ-FIRE-241123/1082
Product: firefox_esr					
Affected Version(s): * Up to (excluding) 115.4					
Out-of-bounds Write	25-Oct-2023	9.8	Memory safety bugs present in Firefox 118, Firefox ESR 115.3, and Thunderbird 115.3. Some of these bugs showed evidence	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/	A-MOZ-FIRE-241123/1083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5730**	mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/	
N/A	25-Oct-2023	7.5	Drivers are not always robust to extremely large draw calls and in some cases this scenario could have led to a crash. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5724**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1836705	A-MOZ-FIRE-241123/1084
N/A	25-Oct-2023	7.5	During garbage collection extra operations were performed on a object that should not be. This could have led to a potentially exploitable crash. This vulnerability affects Firefox < 119, Firefox ESR <	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/,	A-MOZ-FIRE-241123/1085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5728**	https://bugzilla.mozilla.org/show_bug.cgi?id=1852729	
N/A	25-Oct-2023	6.5	The executable file warning was not presented when downloading .msix, .msixbundle, .appx, and .appxbundle files, which can run commands on a user's computer. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.* This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5727**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1847180	A-MOZ-FIRE-241123/1086
Improper Restriction of Rendered UI Layers or Frames	25-Oct-2023	4.3	It was possible for certain browser prompts and dialogs to be activated or dismissed unintentionally by the user due to an insufficient activation-delay. This vulnerability affects Firefox < 119, Firefox ESR <	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla	A-MOZ-FIRE-241123/1087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5721**	.mozilla.org/show_bug.cgi?id=1830820	
N/A	25-Oct-2023	4.3	A malicious installed WebExtension could open arbitrary URLs, which under the right circumstance could be leveraged to collect sensitive user data. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5725**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://bugzilla.mozilla.org/show_bug.cgi?id=1845739, https://www.mozilla.org/security/advisories/mfsa2023-46/	A-MOZ-FIRE-241123/1088
N/A	25-Oct-2023	4.3	A website could have obscured the full screen notification by using the file open dialog. This could have led to user confusion and possible spoofing attacks. *Note: This issue only affected macOS operating systems. Other operating systems are unaffected.* This vulnerability affects Firefox < 119, Firefox ESR <	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1846205	A-MOZ-FIRE-241123/1089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5726**		
Affected Version(s): * Up to (excluding) 115.4.1					
N/A	25-Oct-2023	6.5	An attacker could have created a malicious link using bidirectional characters to spoof the location in the address bar when visited. This vulnerability affects Firefox < 117, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5732**	https://www.mozilla.org/security/advisories/mfsa2023-34/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1690979	A-MOZ-FIRE-241123/1090
Product: thunderbird					
Affected Version(s): * Up to (excluding) 115.4.1					
Out-of-bounds Write	25-Oct-2023	9.8	Memory safety bugs present in Firefox 118, Firefox ESR 115.3, and Thunderbird 115.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/	A-MOZ-THUN-241123/1091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 115.4.1. **CVE ID : CVE-2023-5730**		
N/A	25-Oct-2023	7.5	Drivers are not always robust to extremely large draw calls and in some cases this scenario could have led to a crash. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5724**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1836705	A-MOZ-THUN-241123/1092
N/A	25-Oct-2023	7.5	During garbage collection extra operations were performed on a object that should not be. This could have led to a potentially exploitable crash. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5728**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1852729	A-MOZ-THUN-241123/1093
N/A	25-Oct-2023	6.5	The executable file warning was not presented when downloading .msix, .msixbundle, .appx,	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.m	A-MOZ-THUN-241123/1094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and .appxbundle files, which can run commands on a user's computer. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.* This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5727**	ozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1847180	
N/A	25-Oct-2023	6.5	An attacker could have created a malicious link using bidirectional characters to spoof the location in the address bar when visited. This vulnerability affects Firefox < 117, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5732**	https://www.mozilla.org/security/advisories/mfsa2023-34/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1690979	A-MOZ-THUN-241123/1095
Improper Restriction of Rendered UI Layers or Frames	25-Oct-2023	4.3	It was possible for certain browser prompts and dialogs to be activated or dismissed unintentionally by	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/	A-MOZ-THUN-241123/1096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the user due to an insufficient activation-delay. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5721**	mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1830820	
N/A	25-Oct-2023	4.3	A malicious installed WebExtension could open arbitrary URLs, which under the right circumstance could be leveraged to collect sensitive user data. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5725**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://bugzilla.mozilla.org/show_bug.cgi?id=1845739, https://www.mozilla.org/security/advisories/mfsa2023-46/	A-MOZ-THUN-241123/1097
N/A	25-Oct-2023	4.3	A website could have obscured the full screen notification by using the file open dialog. This could have led to user confusion and possible spoofing attacks. *Note: This issue only affected macOS operating	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/sho	A-MOZ-THUN-241123/1098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			systems. Other operating systems are unaffected.* This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5726**	w_bug.cgi?id=1846205	
Vendor: mpembed					
Product: wp_matterport_shortcode					
Affected Version(s): * Up to (excluding) 2.1.7					
N/A	16-Oct-2023	6.1	The WP Matterport Shortcode WordPress plugin before 2.1.7 does not escape the PHP_SELF server variable when outputting it in attributes, leading to Reflected Cross-Site Scripting issues which could be used against high privilege users such as admin **CVE ID : CVE-2023-4290**	N/A	A-MPE-WP_M-241123/1099
Affected Version(s): * Up to (excluding) 2.1.8					
N/A	16-Oct-2023	5.4	The WP Matterport Shortcode WordPress plugin before 2.1.8 does not validate and escape some of its shortcode attributes before	N/A	A-MPE-WP_M-241123/1100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-4289**		
Vendor: mrpeng					
Product: mpoperationlogs					
Affected Version(s): * Up to (including) 1.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	6.1	The MpOperationLogs plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the IP Request Headers in versions up to, and including, 1.0.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	N/A	A-MRP-MPOP-241123/1101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5538		
Vendor: mullerdigital					
Product: duplicate_theme					
Affected Version(s): * Up to (including) 0.1.6					
Cross-Site Request Forgery (CSRF)	25-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Muller Digital Inc. Duplicate Theme plugin <= 0.1.6 versions. **CVE ID : CVE-2023-46204**	https://patchstack.com/database/vulnerability/duplicate-theme/wordpress-duplicate-theme-plugin-0-1-6-cross-site-request-forgery-csrf-vulnerability?_s_id=cve	A-MUL-DUPL-241123/1102
Vendor: myeventon					
Product: eventon					
Affected Version(s): * Up to (excluding) 2.2					
N/A	16-Oct-2023	4.8	The EventON WordPress plugin before 2.2 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-2023-4388**	N/A	A-MYE-EVEN-241123/1103
Product: eventon-lite					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-2023	6.1	The EventON plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in versions up to, and including, 2.2.2 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-2023-4635**	N/A	A-MYE-EVEN-241123/1104
Vendor: mypresta					
Product: product_extra_tabs_pro					
Affected Version(s): * Up to (excluding) 2.2.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Oct-2023	9.8	In the module extratabspro before version 2.2.8 from MyPresta.eu for PrestaShop, a guest can perform SQL injection via `extratabspro::searchcategory()`, `extratabspro::sear	https://security.friendsofpresta.org/modules/2023/10/12/extratabspro.html	A-MYP-PROD-241123/1105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			chproduct()` and `extratabspro::searchmanufacturer().' **CVE ID : CVE-2023-45386**		
Vendor: myprestamodules					
Product: exportproducts					
Affected Version(s): * Up to (excluding) 5.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Oct-2023	7.5	In the module "Product Catalog (CSV, Excel, XML) Export PRO" (exportproducts) in versions up to 4.1.1 from MyPrestaModules for PrestaShop, a guest can download personal information without restriction by performing a path traversal attack. Due to a lack of permissions control and a lack of control in the path name construction, a guest can perform a path traversal to view all files on the information system. **CVE ID : CVE-2023-46346**	N/A	A-MYP-EXPO-241123/1106
Vendor: myshopkit					
Product: winters					
Affected Version(s): * Up to (including) 1.4.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	6.1	The Winters theme for WordPress is vulnerable to Reflected Cross-Site Scripting via prototype pollution in versions up to, and including, 1.4.3 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-2023-3962**	N/A	A-MYS-WINT-241123/1107
Vendor: Nagvis					
Product: nagvis					
Affected Version(s): * Up to (excluding) 1.9.38					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	6.1	XSS exists in NagVis before 1.9.38 via the select function in share/server/core/functions/html.php. **CVE ID : CVE-2023-46287**	https://github.com/NagVis/nagvis/pull/356/commits/d660591b23e5cfea4d1be2d3fb8f3855aa6020fb	A-NAG-NAGV-241123/1108
Vendor: ndkdesign					
Product: ndk_steppingpack					
Affected Version(s): * Up to (excluding) 1.5.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	9.8	In the module "Step by Step products Pack" (ndk_steppingpack) version 1.5.6 and before from NDK Design for PrestaShop, a guest can perform SQL injection. The method `NdkSpack::getPacks()` has sensitive SQL calls that can be executed with a trivial http call and exploited to forge a SQL injection. **CVE ID : CVE-2023-46347**	N/A	A-NDK-NDK_-241123/1109
Vendor: Netapp					
Product: oncommand_insight					
Affected Version(s): -					
N/A	17-Oct-2023	8.3	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.1.0 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks	https://www.oracle.com/security-alerts/cpuoct2023.html	A-NET-ONCO-241123/1110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			require human interaction from a person other than the attacker and while the vulnerability is in MySQL Connectors, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2023-22102**		
Vendor: netentsec					
Product: application_security_gateway					
Affected Version(s): 6.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Oct-2023	9.8	A vulnerability, which was classified as critical, was found in Netentsec NS-ASG Application Security Gateway 6.3. Affected is an unknown function of the file /protocol/iscgwtunnel/uploadiscgwr	N/A	A-NET-APPL-241123/1111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			outeconf.php. The manipulation of the argument GWLinkId leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-243138 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-5700**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	9.8	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3 and classified as critical. Affected by this issue is some unknown functionality of the file /protocol/firewall/uploadfirewall.php. The manipulation of the argument messagecontent leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-243590 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did	N/A	A-NET-APPL-241123/1112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not respond in any way. **CVE ID : CVE-2023-5784**		
N/A	27-Oct-2023	8.8	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/list_onlineuser.php. The manipulation of the argument SessionId leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-243716. NOTE: We tried to contact the vendor early about the disclosure but the official mail address was not working properly. **CVE ID : CVE-2023-5826**	N/A	A-NET-APPL-241123/1113
Improper Neutralization of Special Elements used in an SQL Command	26-Oct-2023	7.5	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been classified as critical. This affects an unknown part	N/A	A-NET-APPL-241123/1114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			of the file /protocol/firewall/addaddress_interpret.php. The manipulation of the argument messagecontent leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-243591. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-5785**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Oct-2023	7.2	A vulnerability, which was classified as critical, was found in Netentsec NS-ASG Application Security Gateway 6.3. This affects an unknown part of the file /admin/list_addr_fwresource_ip.php. The manipulation leads to sql injection. It is possible to initiate the attack remotely. The	N/A	A-NET-APPL-241123/1115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. The identifier VDB-243057 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-5681**		
Vendor: netmodule					
Product: netmodule_router_software					
Affected Version(s): * Up to (excluding) 4.6.0.105					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Oct-2023	6.6	The web administration interface in NetModule Router Software (NRSW) 4.6 before 4.6.0.106 and 4.8 before 4.8.0.101 executes an OS command constructed with unsanitized user input: shell metacharacters in the /admin/gnssAutoAlign.php device_id parameter. This occurs because another thread can be started before the trap that triggers the cleanup function. A	N/A	A-NET-NETM-241123/1116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow an authenticated user to execute arbitrary commands with elevated privileges. NOTE: this is different from CVE-2023-0861 and CVE-2023-0862, which were fixed in version 4.6.0.105. **CVE ID : CVE-2023-46306**		
Affected Version(s): From (including) 4.7.0.0 Up to (excluding) 4.7.0.103					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Oct-2023	6.6	The web administration interface in NetModule Router Software (NRSW) 4.6 before 4.6.0.106 and 4.8 before 4.8.0.101 executes an OS command constructed with unsanitized user input: shell metacharacters in the /admin/gnssAutoAlign.php device_id parameter. This occurs because another thread can be started before the trap that triggers the cleanup function. A successful exploit could allow an authenticated user	N/A	A-NET-NETM-241123/1117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands with elevated privileges. NOTE: this is different from CVE-2023-0861 and CVE-2023-0862, which were fixed in version 4.6.0.105. **CVE ID : CVE-2023-46306**		
Vendor: networknt					
Product: light-oauth2					
Affected Version(s): * Up to (excluding) 2.1.27					
Improper Certificate Validation	25-Oct-2023	5.9	light-oauth2 before version 2.1.27 obtains the public key without any verification. This could allow attackers to authenticate to the application with a crafted JWT token. **CVE ID : CVE-2023-31580**	N/A	A-NET-LIGH-241123/1118
Vendor: networktocode					
Product: nautobot					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.0.3					
Cleartext Storage of Sensitive Informatio n	25-Oct-2023	6.5	Nautobot is a Network Automation Platform built as a web application atop the Django Python framework with a PostgreSQL or MySQL database. In Nautobot 2.0.x,	https://github.com/nautobot/nautobot/security/advisories/GHSA-r2hw-74xv-4gqp, https://github.com/nautobot/nautobot/pull/4692, https://github.c	A-NET-NAUT-241123/1119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			certain REST API endpoints, in combination with the `?depth=<N>` query parameter, can expose hashed user passwords as stored in the database to any authenticated user with access to these endpoints. The passwords are not exposed in plaintext. This vulnerability has been patched in version 2.0.3. **CVE ID : CVE-2023-46128**	om/nautobot/nautobot/commit/1ce8e5c658a075c29554d517cd453675e5d40d71	
Vendor: Nextcloud					
Product: calendar					
Affected Version(s): From (including) 1.0 Up to (excluding) 4.4.4					
Improper Validation of Integrity Check Value	16-Oct-2023	4.3	Nextcloud calendar is a calendar app for the Nextcloud server platform. Due to missing precondition checks the server was trying to validate strings of any length as email addresses even when megabytes of data were provided, eventually making the server busy and unresponsive. It is recommended that the Nextcloud	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-r936-8gwm-w452, https://github.com/nextcloud/calendar/pull/5358	A-NEX-CALE-241123/1120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Calendar app is upgraded to 4.4.4. The only workaround for users unable to upgrade is to disable the calendar app. **CVE ID : CVE-2023-45150**		
Product: mail					
Affected Version(s): From (including) 2.2.0 Up to (excluding) 2.2.8					
Server-Side Request Forgery (SSRF)	16-Oct-2023	4.3	Nextcloud mail is an email app for the Nextcloud home server platform. In affected versions a missing check of origin, target and cookies allows for an attacker to abuse the proxy endpoint to denial of service a third server. It is recommended that the Nextcloud Mail is upgraded to 2.2.8 or 3.3.0. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45660**	https://github.com/nextcloud/mail/pull/8459, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-8j9x-fmww-qr37	A-NEX-MAIL-241123/1121
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.3.0					
Server-Side Request	16-Oct-2023	4.3	Nextcloud mail is an email app for the Nextcloud home server platform. In	https://github.com/nextcloud/mail/pull/8459, https://github.com/nextcloud/s	A-NEX-MAIL-241123/1122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			affected versions a missing check of origin, target and cookies allows for an attacker to abuse the proxy endpoint to denial of service a third server. It is recommended that the Nextcloud Mail is upgraded to 2.2.8 or 3.3.0. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45660**	ecurity-advisories/security/advisories/GHSA-8j9x-fmww-qr37	
Product: nextcloud_server					
Affected Version(s): 27.0.0					
Cleartext Storage of Sensitive Informatio n	16-Oct-2023	8.8	Nextcloud server is an open source home cloud platform. Affected versions of Nextcloud stored OAuth2 tokens in plaintext which allows an attacker who has gained access to the server to potentially elevate their privilege. This issue has been addressed and users are recommended to upgrade their Nextcloud Server to version 25.0.8, 26.0.3 or 27.0.1.	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-hhgv-jcg9-p4m9, https://github.com/nextcloud/server/pull/38398	A-NEX-NEXT-241123/1123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45151**		
Improper Restriction of Excessive Authentication Attempts	16-Oct-2023	4.3	Nextcloud is an open source home cloud server. When Memcached is used as `memcache.distributed` the rate limiting in Nextcloud Server could be reset unexpectedly resetting the rate count earlier than intended. Users are advised to upgrade to versions 25.0.11, 26.0.6 or 27.1.0. Users unable to upgrade should change their config setting `memcache.distributed` to `\OC\Memcache\Redis` and install Redis instead of Memcached. **CVE ID : CVE-2023-45148**	https://github.com/nextcloud/server/pull/40293, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-xmhp-7vr4-hp63	A-NEX-NEXT-241123/1124
Affected Version(s): From (including) 22.0.0 Up to (excluding) 22.2.10.16					
Improper Restriction of Excessive Authentica	16-Oct-2023	4.3	Nextcloud is an open source home cloud server. When Memcached is used as `memcache.distrib	https://github.com/nextcloud/server/pull/40293, https://github.com/nextcloud/s	A-NEX-NEXT-241123/1125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion Attempts			uted` the rate limiting in Nextcloud Server could be reset unexpectedly resetting the rate count earlier than intended. Users are advised to upgrade to versions 25.0.11, 26.0.6 or 27.1.0. Users unable to upgrade should change their config setting `memcache.distributed` to `\OC\Memcache\Redis` and install Redis instead of Memcached. **CVE ID : CVE-2023-45148**	ecurity-advisories/security/advisories/GHSA-xmhp-7vr4-hp63	
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.0.12.11					
Improper Restriction of Excessive Authentication Attempts	16-Oct-2023	4.3	Nextcloud is an open source home cloud server. When Memcached is used as `memcache.distributed` the rate limiting in Nextcloud Server could be reset unexpectedly resetting the rate count earlier than intended. Users are advised to upgrade to versions 25.0.11, 26.0.6 or 27.1.0. Users unable to upgrade should	https://github.com/nextcloud/server/pull/40293, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-xmhp-7vr4-hp63	A-NEX-NEXT-241123/1126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			change their config setting `memcache.distributed` to `\OC\Memcache\Redis` and install Redis instead of Memcached. **CVE ID : CVE-2023-45148**		
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.12.7					
Improper Restriction of Excessive Authentication Attempts	16-Oct-2023	4.3	Nextcloud is an open source home cloud server. When Memcached is used as `memcache.distributed` the rate limiting in Nextcloud Server could be reset unexpectedly resetting the rate count earlier than intended. Users are advised to upgrade to versions 25.0.11, 26.0.6 or 27.1.0. Users unable to upgrade should change their config setting `memcache.distributed` to `\OC\Memcache\Redis` and install Redis instead of Memcached. **CVE ID : CVE-2023-45148**	https://github.com/nextcloud/server/pull/40293, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-xmhp-7vr4-hp63	A-NEX-NEXT-241123/1127
Affected Version(s): From (including) 25.0.0 Up to (excluding) 25.0.11					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	16-Oct-2023	4.3	Nextcloud is an open source home cloud server. When Memcached is used as `memcache.distributed` the rate limiting in Nextcloud Server could be reset unexpectedly resetting the rate count earlier than intended. Users are advised to upgrade to versions 25.0.11, 26.0.6 or 27.1.0. Users unable to upgrade should change their config setting `memcache.distributed` to `\OC\Memcache\Redis` and install Redis instead of Memcached. **CVE ID : CVE-2023-45148**	https://github.com/nextcloud/server/pull/40293, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-xmhp-7vr4-hp63	A-NEX-NEXT-241123/1128
Affected Version(s): From (including) 25.0.0 Up to (excluding) 25.0.8					
Cleartext Storage of Sensitive Information	16-Oct-2023	8.8	Nextcloud server is an open source home cloud platform. Affected versions of Nextcloud stored OAuth2 tokens in plaintext which allows an attacker who has gained access to the server to potentially elevate their	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-hhgv-jcg9-p4m9, https://github.com/nextcloud/server/pull/38398	A-NEX-NEXT-241123/1129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege. This issue has been addressed and users are recommended to upgrade their Nextcloud Server to version 25.0.8, 26.0.3 or 27.0.1. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45151**		
Affected Version(s): From (including) 26.0.0 Up to (excluding) 26.0.3					
Cleartext Storage of Sensitive Information	16-Oct-2023	8.8	Nextcloud server is an open source home cloud platform. Affected versions of Nextcloud stored OAuth2 tokens in plaintext which allows an attacker who has gained access to the server to potentially elevate their privilege. This issue has been addressed and users are recommended to upgrade their Nextcloud Server to version 25.0.8, 26.0.3 or 27.0.1. There are no known workarounds for this vulnerability.	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-hhgv-jcg9-p4m9, https://github.com/nextcloud/server/pull/38398	A-NEX-NEXT-241123/1130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45151		
Affected Version(s): From (including) 26.0.0 Up to (excluding) 26.0.6					
Improper Restriction of Excessive Authentication Attempts	16-Oct-2023	4.3	Nextcloud is an open source home cloud server. When Memcached is used as `memcache.distributed` the rate limiting in Nextcloud Server could be reset unexpectedly resetting the rate count earlier than intended. Users are advised to upgrade to versions 25.0.11, 26.0.6 or 27.1.0. Users unable to upgrade should change their config setting `memcache.distributed` to `\OC\Memcache\Redis` and install Redis instead of Memcached. **CVE ID : CVE-2023-45148**	https://github.com/nextcloud/server/pull/40293, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-xmhp-7vr4-hp63	A-NEX-NEXT-241123/1131
Product: talk					
Affected Version(s): From (including) 15.0.0 Up to (excluding) 15.0.8					
Improper Restriction of Excessive Authentication Attempts	16-Oct-2023	4.3	Nextcloud talk is a chat module for the Nextcloud server platform. In affected versions brute force protection of public talk	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-7rf8-pqmj-rpqv, https://github.c	A-NEX-TALK-241123/1132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conversation passwords can be bypassed, as there was an endpoint validating the conversation password without registering bruteforce attempts. It is recommended that the Nextcloud Talk app is upgraded to 15.0.8, 16.0.6 or 17.1.1. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45149**	om/nextcloud/spreed/pull/10545	
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.0.6					
Improper Restriction of Excessive Authentication Attempts	16-Oct-2023	4.3	Nextcloud talk is a chat module for the Nextcloud server platform. In affected versions brute force protection of public talk conversation passwords can be bypassed, as there was an endpoint validating the conversation password without registering bruteforce attempts. It is recommended that the Nextcloud Talk app is upgraded to 15.0.8, 16.0.6 or	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-7rf8-pqmj-rpqv, https://github.com/nextcloud/spreed/pull/10545	A-NEX-TALK-241123/1133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			17.1.1. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45149**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.1					
Improper Restriction of Excessive Authentication Attempts	16-Oct-2023	4.3	Nextcloud talk is a chat module for the Nextcloud server platform. In affected versions brute force protection of public talk conversation passwords can be bypassed, as there was an endpoint validating the conversation password without registering bruteforce attempts. It is recommended that the Nextcloud Talk app is upgraded to 15.0.8, 16.0.6 or 17.1.1. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45149**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-7rf8-pqmj-rpqv, https://github.com/nextcloud/spreed/pull/10545	A-NEX-TALK-241123/1134
Vendor: nextgen					
Product: mirth_connect					
Affected Version(s): * Up to (excluding) 4.4.1					
N/A	26-Oct-2023	9.8	NextGen Healthcare Mirth Connect before	N/A	A-NEX-MIRT-241123/1135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 4.4.1 is vulnerable to unauthenticated remote code execution. Note that this vulnerability is caused by the incomplete patch of CVE-2023-37679. **CVE ID : CVE-2023-43208**		
Vendor: NI					
Product: system_configuration					
Affected Version(s): * Up to (excluding) 2023					
Out-of-bounds Write	18-Oct-2023	9.8	A stack-based buffer overflow vulnerability exists in NI System Configuration that could result in information disclosure and/or arbitrary code execution. Successful exploitation requires that an attacker can provide a specially crafted response. This affects NI System Configuration 2023 Q3 and all previous versions. **CVE ID : CVE-2023-4601**	https://www.ni.com/en/support/documentation/supplemental/23/stack-based-buffer-overflow-in-ni-system-configuration.html	A-NI-SYST-241123/1136
Affected Version(s): 2023					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Oct-2023	9.8	A stack-based buffer overflow vulnerability exists in NI System Configuration that could result in information disclosure and/or arbitrary code execution. Successful exploitation requires that an attacker can provide a specially crafted response. This affects NI System Configuration 2023 Q3 and all previous versions. **CVE ID : CVE-2023-4601**	https://www.ni.com/en/support/documentation/supplemental/23/stack-based-buffer-overflow-in-ni-system-configuration.html	A-NI-SYST-241123/1137
Vendor: nic					
Product: knot_resolver					
Affected Version(s): * Up to (excluding) 5.7.0					
N/A	22-Oct-2023	7.5	Knot Resolver before 5.7.0 performs many TCP reconnections upon receiving certain nonsensical responses from servers. **CVE ID : CVE-2023-46317**	https://gitlab.nic.cz/knot/knot-resolver/-/merge_requests/1448	A-NIC-KNOT-241123/1138
Vendor: nicolamodugno					
Product: smart_cookie_kit					
Affected Version(s): * Up to (excluding) 2.3.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Nicola Modugno Smart Cookie Kit plugin <= 2.3.1 versions. **CVE ID : CVE-2023-45608**	N/A	A-NIC-SMAR-241123/1139
Vendor: ninjateam					
Product: filester					
Affected Version(s): * Up to (excluding) 1.8					
N/A	16-Oct-2023	8.8	The File Manager Pro WordPress plugin before 1.8 does not properly check the CSRF nonce in the `fs_connector` AJAX action. This allows attackers to make highly privileged users perform unwanted file system actions via CSRF attacks by using GET requests, such as uploading a web shell. **CVE ID : CVE-2023-4827**	N/A	A-NIN-FILE-241123/1140
Affected Version(s): * Up to (excluding) 1.8.1					
N/A	16-Oct-2023	7.2	The File Manager Pro WordPress plugin before 1.8.1 allows admin users to upload arbitrary files, even in	N/A	A-NIN-FILE-241123/1141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			environments where such a user should not be able to gain full control of the server, such as a multisite installation. This leads to remote code execution. **CVE ID : CVE-2023-4861**		
N/A	16-Oct-2023	4.8	The File Manager Pro WordPress plugin before 1.8.1 does not adequately validate and escape some inputs, leading to XSS by high-privilege users. **CVE ID : CVE-2023-4862**	N/A	A-NIN-FILE-241123/1142
Product: live_chat_with_facebook_messenger					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	The Live Chat with Facebook Messenger plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'messenger' shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it	N/A	A-NIN-LIVE-241123/1143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5740**		
Vendor: Nodejs					
Product: node.js					
Affected Version(s): * Up to (excluding) 20.8.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-2023	9.8	Various `node:fs` functions allow specifying paths as either strings or `Uint8Array` objects. In Node.js environments, the `Buffer` class extends the `Uint8Array` class. Node.js prevents path traversal through strings (see CVE-2023-30584) and `Buffer` objects (see CVE-2023-32004), but not through non-`Buffer` `Uint8Array` objects. This is distinct from CVE-2023-32004 which only	N/A	A-NOD-NODE-241123/1144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			referred to `Buffer` objects. However, the vulnerability follows the same pattern using `Uint8Array` instead of `Buffer`. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. **CVE ID : CVE-2023-39332**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Oct-2023	7.5	A previously disclosed vulnerability (CVE-2023-30584) was patched insufficiently in commit 205f1e6. The new path traversal vulnerability arises because the implementation does not protect itself against the application overwriting built-in utility functions with user-defined implementations. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. **CVE ID : CVE-2023-39331**	N/A	A-NOD-NODE-241123/1145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 18.0.0 Up to (including) 18.18.1					
Insufficient Verification of Data Authenticity	18-Oct-2023	7.5	When the Node.js policy feature checks the integrity of a resource against a trusted manifest, the application can intercept the operation and return a forged checksum to the node's policy implementation, thus effectively disabling the integrity check. Impacts: This vulnerability affects all users using the experimental policy mechanism in all active release lines: 18.x and, 20.x. Please note that at the time this CVE was issued, the policy mechanism is an experimental feature of Node.js. **CVE ID : CVE-2023-38552**	N/A	A-NOD-NODE-241123/1146
Affected Version(s): From (including) 20.1.0 Up to (including) 20.8.0					
Insufficient Verification of Data Authenticity	18-Oct-2023	7.5	When the Node.js policy feature checks the integrity of a resource against a trusted manifest, the application can	N/A	A-NOD-NODE-241123/1147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intercept the operation and return a forged checksum to the node's policy implementation, thus effectively disabling the integrity check. Impacts: This vulnerability affects all users using the experimental policy mechanism in all active release lines: 18.x and, 20.x. Please note that at the time this CVE was issued, the policy mechanism is an experimental feature of Node.js. **CVE ID : CVE-2023-38552**		
Vendor: northernbeacheswebsites					
Product: gotowebinar					
Affected Version(s): * Up to (including) 14.45					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Martin Gibson WP GoToWebinar plugin <= 14.45 versions. **CVE ID : CVE-2023-45832**	N/A	A-NOR-GOTO-241123/1148
Vendor: northgrid					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: proself					
Affected Version(s): * Up to (excluding) 1.09					
Improper Restriction of XML External Entity Reference	18-Oct-2023	7.5	Proself Enterprise/Standard Edition Ver5.62 and earlier, Proself Gateway Edition Ver1.65 and earlier, and Proself Mail Sanitize Edition Ver1.08 and earlier allow a remote unauthenticated attacker to conduct XML External Entity (XXE) attacks. By processing a specially crafted request containing malformed XML data, arbitrary files on the server containing account information may be read by the attacker. **CVE ID : CVE-2023-45727**	https://www.proself.jp/information/153/	A-NOR-PROS-241123/1149
Affected Version(s): * Up to (excluding) 1.66					
Improper Restriction of XML External Entity Reference	18-Oct-2023	7.5	Proself Enterprise/Standard Edition Ver5.62 and earlier, Proself Gateway Edition Ver1.65 and earlier, and Proself Mail Sanitize Edition Ver1.08 and earlier allow a remote	https://www.proself.jp/information/153/	A-NOR-PROS-241123/1150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to conduct XML External Entity (XXE) attacks. By processing a specially crafted request containing malformed XML data, arbitrary files on the server containing account information may be read by the attacker. **CVE ID : CVE-2023-45727**		
Affected Version(s): * Up to (excluding) 5.63					
Improper Restriction of XML External Entity Reference	18-Oct-2023	7.5	Proself Enterprise/Standard Edition Ver5.62 and earlier, Proself Gateway Edition Ver1.65 and earlier, and Proself Mail Sanitize Edition Ver1.08 and earlier allow a remote unauthenticated attacker to conduct XML External Entity (XXE) attacks. By processing a specially crafted request containing malformed XML data, arbitrary files on the server containing account information may	https://www.proself.jp/information/153/	A-NOR-PROS-241123/1151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be read by the attacker. **CVE ID : CVE-2023-45727**		
Vendor: nothings					
Product: stb_image.h					
Affected Version(s): 2.28					
Double Free	21-Oct-2023	9.8	stb_image is a single file MIT licensed library for processing images. It may look like `stbi__load_gif_main` doesn't give guarantees about the content of output value `*delays` upon failure. Although it sets `*delays` to zero at the beginning, it doesn't do it in case the image is not recognized as GIF and a call to `stbi__load_gif_main_outofmem` only frees possibly allocated memory in `*delays` without resetting it to zero. Thus it would be fair to say the caller of `stbi__load_gif_main` is responsible to free the allocated memory in `*delays` only if `stbi__load_gif_main` returns a non	N/A	A-NOT-STB_-241123/1152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			null value. However at the same time the function may return null value, but fail to free the memory in `*delays` if internally `stbi__convert_format` is called and fails. Thus the issue may lead to a memory leak if the caller chooses to free `delays` only when `stbi__load_gif_main` didn't fail or to a double-free if the `delays` is always freed **CVE ID : CVE-2023-45666**		
Double Free	21-Oct-2023	8.8	stb_image is a single file MIT licensed library for processing images. A crafted image file can trigger `stbi__load_gif_main_outofmem` attempt to double-free the out variable. This happens in `stbi__load_gif_main` because when the `layers * stride` value is zero the behavior is implementation defined, but	N/A	A-NOT-STB_-241123/1153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			common that realloc frees the old memory and returns null pointer. Since it attempts to double-free the memory a few lines below the first "free", the issue can be potentially exploited only in a multi-threaded environment. In the worst case this may lead to code execution. **CVE ID : CVE-2023-45664**		
Out-of-bounds Read	21-Oct-2023	8.1	stb_image is a single file MIT licensed library for processing images. When `stbi_set_flip_vertically_on_load` is set to `TRUE` and `req_comp` is set to a number that doesn't match the real number of components per pixel, the library attempts to flip the image vertically. A crafted image file can trigger `memcpy` out-of-bounds read because `bytes_per_pixel` used to calculate `bytes_per_row`	N/A	A-NOT-STB_-241123/1154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			doesn't match the real image array dimensions. **CVE ID : CVE-2023-45662**		
NULL Pointer Dereference	21-Oct-2023	7.5	stb_image is a single file MIT licensed library for processing images. If `stbi__load_gif_main` in `stbi_load_gif_from_memory` fails it returns a null pointer and may keep the `z` variable uninitialized. In case the caller also sets the flip vertically flag, it continues and calls `stbi__vertical_flip_slices` with the null pointer result value and the uninitialized `z` value. This may result in a program crash. **CVE ID : CVE-2023-45667**	N/A	A-NOT-STB_-241123/1155
Out-of-bounds Read	21-Oct-2023	7.1	stb_image is a single file MIT licensed library for processing images. A crafted image file may trigger out of bounds memcpy read in	https://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_image.h#L6817	A-NOT-STB_-241123/1156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`stbi__gif_load_next `. This happens because two_back points to a memory address lower than the start of the buffer out. This issue may be used to leak internal memory allocation information. **CVE ID : CVE-2023-45661**		
Double Free	25-Oct-2023	6.5	Double Free vulnerability in Nothings Stb Image.h v.2.28 allows a remote attacker to cause a denial of service via a crafted file to the stbi_load_gif_main function. **CVE ID : CVE-2023-43281**	N/A	A-NOT-STB_-241123/1157
Use of Uninitialized Resource	21-Oct-2023	5.5	stb_image is a single file MIT licensed library for processing images. The stbi__getn function reads a specified number of bytes from context (typically a file) into the specified buffer. In case the file stream points to the end, it returns zero. There are two places where its return value is not	N/A	A-NOT-STB_-241123/1158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checked: In the `stbi__hdr_load` function and in the `stbi__tga_load` function. The latter of the two is likely more exploitable as an attacker may also control the size of an uninitialized buffer. **CVE ID : CVE-2023-45663**		
Product: stb_vorbis.c					
Affected Version(s): 1.22					
Out-of-bounds Write	21-Oct-2023	7.8	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger out of bounds write in `f->vendor[len] = (char)'\0';`. The root cause is that if the len read in `start_decoder` is `-1` and `len + 1` becomes 0 when passed to `setup_malloc`. The `setup_malloc` behaves differently when `f->alloc.alloc_buffer` is pre-allocated. Instead of returning `NULL` as in `malloc` case it shifts the pre-allocated buffer by	N/A	A-NOT-STB_-241123/1159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			zero and returns the currently available memory block. This issue may lead to code execution. **CVE ID : CVE-2023-45675**		
Out-of-bounds Write	21-Oct-2023	7.8	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger out of bounds write in `f->vendor[i] = get8_packet(f);`. The root cause is an integer overflow in `setup_malloc`. A sufficiently large value in the variable `sz` overflows with `sz+7` in and the negative value passes the maximum available memory buffer check. This issue may lead to code execution. **CVE ID : CVE-2023-45676**	N/A	A-NOT-STB_-241123/1160
Out-of-bounds Write	21-Oct-2023	7.8	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger out of bounds write in `f-	N/A	A-NOT-STB_-241123/1161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			>vendor[len] = (char)'\0';`. The root cause is that if `len` read in `start_decoder` is a negative number and `setup_malloc` successfully allocates memory in that case, but memory write is done with a negative index `len`. Similarly if len is INT_MAX the integer overflow len+1 happens in `f->vendor = (char*)setup_malloc(f, sizeof(char) * (len+1));` and `f->comment_list[i] = (char*)setup_malloc(f, sizeof(char) * (len+1));`. This issue may lead to code execution. **CVE ID : CVE-2023-45677**		
Out-of-bounds Write	21-Oct-2023	7.8	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger out of buffer write in `start_decoder` because at maximum `m->submaps` can be 16 but `submap_floor` and	N/A	A-NOT-STB_-241123/1162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`submap_residue` are declared as arrays of 15 elements. This issue may lead to code execution. **CVE ID : CVE-2023-45678**		
Double Free	21-Oct-2023	7.8	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger memory allocation failure in `start_decoder`. In that case the function returns early, but some of the pointers in `f->comment_list` are left initialized and later `setup_free` is called on these pointers in `vorbis_deinit`. This issue may lead to code execution. **CVE ID : CVE-2023-45679**	N/A	A-NOT-STB_-241123/1163
Integer Overflow or Wraparound	21-Oct-2023	7.8	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger memory write past an allocated heap buffer in `start_decoder`. The root cause is a	N/A	A-NOT-STB_-241123/1164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential integer overflow in `sizeof(char*) * (f->comment_list_length)` which may make `setup_malloc` allocate less memory than required. Since there is another integer overflow an attacker may overflow it too to force `setup_malloc` to return 0 and make the exploit more reliable. This issue may lead to code execution. **CVE ID : CVE-2023-45681**		
Out-of-bounds Read	21-Oct-2023	7.1	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger out of bounds read in `DECODE` macro when `var` is negative. As it can be seen in the definition of `DECODE_RAW` a negative `var` is a valid value. This issue may be used to leak internal memory allocation information.	N/A	A-NOT-STB_-241123/1165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45682		
NULL Pointer Dereference	21-Oct-2023	5.5	stb_vorbis is a single file MIT licensed library for processing ogg vorbis files. A crafted file may trigger memory allocation failure in `start_decoder`. In that case the function returns early, the `f->comment_list` is set to `NULL`, but `f->comment_list_length` is not reset. Later in `vorbis_deinit` it tries to dereference the `NULL` pointer. This issue may lead to denial of service. **CVE ID : CVE-2023-45680**	N/A	A-NOT-STB_-241123/1166
Vendor: novo-media					
Product: novo-map					
Affected Version(s): your_wp_posts_on_custom_google_maps Up to (including) 1.1.2					
Cross-Site Request Forgery (CSRF)	25-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Novo-media Novo-Map : your WP posts on custom google maps plugin <= 1.1.2 versions. **CVE ID : CVE-2023-46190**	N/A	A-NOV-NOVO-241123/1167
Vendor: obl.ong					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: admin					
Affected Version(s): * Up to (excluding) 1.1.2					
Incorrect Authorization	26-Oct-2023	5.3	The admin panel for Obl.ong before 1.1.2 allows authorization bypass because the email OTP feature accepts arbitrary numerical values. **CVE ID : CVE-2023-46754**	N/A	A-OBL-ADMI-241123/1168
Vendor: ocomon_project					
Product: ocomon					
Affected Version(s): * Up to (excluding) 4.0.1					
Inclusion of Functionality from Untrusted Control Sphere	26-Oct-2023	8.8	A local file inclusion vulnerability via the lang parameter in OcoMon before v4.0.1 allows attackers to execute arbitrary code by supplying a crafted PHP file. **CVE ID : CVE-2023-33559**	N/A	A-OCO-OCOM-241123/1169
N/A	26-Oct-2023	7.5	An information disclosure vulnerability in the component users-grid-data.php of Ocomon before v4.0.1 allows attackers to obtain sensitive information such as e-mails and usernames.	https://github.com/ninj4c0d3r/OcoMon-Research/commit/6357def478b11119270b89329fceb115f12c69fc	A-OCO-OCOM-241123/1170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33558		
Vendor: omrom					
Product: cx-designer					
Affected Version(s): * Up to (including) 3.740					
Improper Restriction of XML External Entity Reference	23-Oct-2023	5.5	CX-Designer Ver.3.740 and earlier (included in CX-One CXONE-AL[][]D-V4) contains an improper restriction of XML external entity reference (XXE) vulnerability. If a user opens a specially crafted project file created by an attacker, sensitive information in the file system where CX-Designer is installed may be disclosed. **CVE ID : CVE-2023-43624**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-011_en.pdf	A-OMR-CX-D-241123/1171
Vendor: onworks					
Product: xolo_cms					
Affected Version(s): 0.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2023	6.1	Xolo CMS v0.11 was discovered to contain a reflected cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2023-43906**	N/A	A-ONW-XOLO-241123/1172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: opencrx					
Product: opencrx					
Affected Version(s): 5.2.2					
Improper Restriction of XML External Entity Reference	30-Oct-2023	9.8	An issue in openCRX v.5.2.2 allows a remote attacker to read internal files and execute server side request forgery attack via insecure DocumentBuilderFactory. **CVE ID : CVE-2023-46502**	https://github.com/opencrx/opencrx/commit/ce7a71db0bb34ecbcb0e822d40598e410a48b399	A-OPE-OPEN-241123/1173
Vendor: openfga					
Product: openfga					
Affected Version(s): * Up to (excluding) 1.3.4					
Uncontrolled Resource Consumption	17-Oct-2023	7.5	OpenFGA is a flexible authorization/permission engine built for developers and inspired by Google Zanzibar. Affected versions of OpenFGA are vulnerable to a denial of service attack. When a number of `ListObjects` calls are executed, in some scenarios, those calls are not releasing resources even after a response has been sent, and given a sufficient call	N/A	A-OPE-OPEN-241123/1174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			volume the service as a whole becomes unresponsive. This issue has been addressed in version 1.3.4 and the upgrade is considered backwards compatible. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45810**		
Vendor: openimageio					
Product: openimageio					
Affected Version(s): 2.4.12.0					
Integer Overflow or Wraparound	23-Oct-2023	8.8	An issue in OpenImageIO oiio v.2.4.12.0 allows a remote attacker to execute arbitrary code and cause a denial of service via the read_rle_image function of file bifs/unquantize.c **CVE ID : CVE-2023-42295**	N/A	A-OPE-OPEN-241123/1175
Vendor: Opensolution					
Product: quick_cms					
Affected Version(s): 6.7					
Improper Neutralization of Input During Web Page	19-Oct-2023	8.6	Cross-site scripting (XSS) vulnerability in opensolution Quick CMS v.6.7 allows a local attacker to execute	N/A	A-OPE-QUIC-241123/1176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			arbitrary code via a crafted script to the Content - Name parameter in the Pages Menu component. **CVE ID : CVE-2023-43345**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2023	5.4	Cross-site scripting (XSS) vulnerability in opensolution Quick CMS v.6.7 allows a local attacker to execute arbitrary code via a crafted script to the Languages Menu component. **CVE ID : CVE-2023-43342**	N/A	A-OPE-QUIC-241123/1177
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2023	5.4	Cross-site scripting (XSS) vulnerability in opensolution Quick CMS v.6.7 allows a local attacker to execute arbitrary code via a crafted script to the SEO - Meta description parameter in the Pages Menu component. **CVE ID : CVE-2023-43344**	N/A	A-OPE-QUIC-241123/1178
Improper Neutralization of Input During Web Page Generation	20-Oct-2023	5.4	Cross-site scripting (XSS) vulnerability in opensolution Quick CMS v.6.7 allows a local attacker to execute arbitrary code via a	N/A	A-OPE-QUIC-241123/1179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			crafted script to the Backend - Dashboard parameter in the Languages Menu component. **CVE ID : CVE-2023-43346**		
Vendor: opnsense					
Product: opnsense					
Affected Version(s): 23.1					
Improper Restriction of Excessive Authentication Attempts	23-Oct-2023	9.8	DECISO OPNsense 23.1 does not impose rate limits for authentication, allowing attackers to perform a brute-force attack to bypass authentication. **CVE ID : CVE-2023-27152**	N/A	A-OPN-OPNS-241123/1180
Vendor: Oracle					
Product: banking_trade_finance					
Affected Version(s): From (including) 14.5 Up to (including) 14.7					
N/A	17-Oct-2023	5.9	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 14.5-14.7. Difficult to exploit vulnerability allows low privileged attacker with network	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-BANK-241123/1181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access via HTTP to compromise Oracle Banking Trade Finance. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Trade Finance accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Trade Finance accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Trade Finance. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:L).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22122		
N/A	17-Oct-2023	5.4	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 14.5-14.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Banking Trade Finance. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Trade Finance accessible data as well as unauthorized read access to a subset of Oracle Banking Trade Finance accessible data. CVSS 3.1 Base	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-BANK-241123/1182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-22121**		
N/A	17-Oct-2023	5.4	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 14.5-14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Trade Finance. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Banking Trade Finance, attacks may significantly impact additional products (scope change).	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-BANK-241123/1183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Trade Finance accessible data as well as unauthorized read access to a subset of Oracle Banking Trade Finance accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22123**		
N/A	17-Oct-2023	5.4	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 14.5-14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-BANK-241123/1184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle Banking Trade Finance. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Banking Trade Finance, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Trade Finance accessible data as well as unauthorized read access to a subset of Oracle Banking Trade Finance accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22124**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Oct-2023	5.4	Vulnerability in the Oracle Banking Trade Finance product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 14.5-14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Trade Finance. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Banking Trade Finance, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Trade Finance accessible data as well as unauthorized read	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-BANK-241123/1185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to a subset of Oracle Banking Trade Finance accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22125**		
Product: bi_publisher					
Affected Version(s): 6.4.0.0.0					
N/A	17-Oct-2023	5.4	Vulnerability in the BI Publisher product of Oracle Analytics (component: Web Server). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher,	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-BI_P-241123/1186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of BI Publisher accessible data as well as unauthorized read access to a subset of BI Publisher accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22105**		
Affected Version(s): 7.0.0.0.0					
N/A	17-Oct-2023	5.4	Vulnerability in the BI Publisher product of Oracle Analytics (component: Web Server). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. Easily exploitable vulnerability allows low	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-BI_P-241123/1187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker with network access via HTTP to compromise BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of BI Publisher accessible data as well as unauthorized read access to a subset of BI Publisher accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22105**		
Product: business_intelligence					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 6.4.0.0.0					
N/A	17-Oct-2023	5.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Pod Admin). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-BUSI-241123/1188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22082**		
N/A	17-Oct-2023	4.6	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web Dashboards). Supported versions that are affected are 6.4.0.0.0, 7.0.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-BUSI-241123/1189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-22109**		
Affected Version(s): 7.0.0.0.0					
N/A	17-Oct-2023	5.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-BUSI-241123/1190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Analytics (component: Pod Admin). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22082**		
N/A	17-Oct-2023	4.6	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web Dashboards). Supported versions that are affected are 6.4.0.0.0, 7.0.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-BUSI-241123/1191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-22109**		
Affected Version(s): 12.2.1.4.0					
N/A	17-Oct-2023	4.6	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web Dashboards). Supported versions that are affected	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-BUSI-241123/1192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are 6.4.0.0.0, 7.0.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/A		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			C:L/PR:L/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-22109**		
Product: commerce_guided_search					
Affected Version(s): 11.3.2					
N/A	17-Oct-2023	6.1	Vulnerability in the Oracle Commerce Guided Search product of Oracle Commerce (component: Workbench). The supported version that is affected is 11.3.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-COMM-241123/1193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			update, insert or delete access to some of Oracle Commerce Guided Search accessible data as well as unauthorized read access to a subset of Oracle Commerce Guided Search accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22029**		
Product: communications_order_and_service_management					
Affected Version(s): 7.4.0					
N/A	17-Oct-2023	4.3	Vulnerability in the Oracle Communications Order and Service Management product of Oracle Communications Applications (component: User Management). Supported versions that are affected are 7.4.0 and 7.4.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-COMM-241123/1194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle Communications Order and Service Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Communications Order and Service Management accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22088**		
Affected Version(s): 7.4.1					
N/A	17-Oct-2023	4.3	Vulnerability in the Oracle Communications Order and Service Management product of Oracle Communications Applications (component: User Management). Supported versions that are affected are 7.4.0 and 7.4.1. Easily exploitable vulnerability allows low privileged attacker with network	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-COMM-241123/1195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access via HTTP to compromise Oracle Communications Order and Service Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Communications Order and Service Management accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22088**		
Product: database_server					
Affected Version(s): From (including) 19.3 Up to (including) 19.20					
N/A	17-Oct-2023	5.9	Vulnerability in the PL/SQL component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows high privileged attacker having Create Session, Execute on sys.utl_http privilege with	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-DATA-241123/1196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network access via Oracle Net to compromise PL/SQL. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PL/SQL, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PL/SQL accessible data as well as unauthorized read access to a subset of PL/SQL accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PL/SQL. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22071		
N/A	17-Oct-2023	4.9	Vulnerability in the Oracle Database Recovery Manager component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows high privileged attacker having DBA account privilege with network access via Oracle Net to compromise Oracle Database Recovery Manager. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Database Recovery Manager. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22077**	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-DATA-241123/1197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Oct-2023	4.3	Vulnerability in the Oracle Notification Server component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Notification Server executes to compromise Oracle Notification Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Notification Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22073**	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-DATA-241123/1198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Oct-2023	4.3	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java VM accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22096**	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-DATA-241123/1199
N/A	17-Oct-2023	2.4	Vulnerability in the Oracle Database Sharding component of Oracle Database	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-DATA-241123/1200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows high privileged attacker having Create Session, Select Any Dictionary privilege with network access via Oracle Net to compromise Oracle Database Sharding. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Database Sharding. CVSS 3.1 Base Score 2.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22074**		
N/A	17-Oct-2023	2.4	Vulnerability in the Oracle Database	https://www.oracle.com/securi	A-ORA-DATA-241123/1201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sharding component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows high privileged attacker having Create Session, Create Any View, Select Any Table privilege with network access via Oracle Net to compromise Oracle Database Sharding. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Database Sharding. CVSS 3.1 Base Score 2.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:L).	ty-alerts/cpuoct2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22075		
Affected Version(s): From (including) 21.3 Up to (including) 21.11					
N/A	17-Oct-2023	5.9	Vulnerability in the PL/SQL component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows high privileged attacker having Create Session, Execute on sys.utl_http privilege with network access via Oracle Net to compromise PL/SQL. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PL/SQL, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PL/SQL accessible data as well as	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-DATA-241123/1202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized read access to a subset of PL/SQL accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PL/SQL. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L). **CVE ID : CVE-2023-22071**		
N/A	17-Oct-2023	4.9	Vulnerability in the Oracle Database Recovery Manager component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows high privileged attacker having DBA account privilege with network access via Oracle Net to compromise Oracle Database Recovery Manager. Successful attacks	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-DATA-241123/1203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Database Recovery Manager. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22077**		
N/A	17-Oct-2023	4.3	Vulnerability in the Oracle Notification Server component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Notification Server executes to compromise Oracle Notification Server.	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-DATA-241123/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Notification Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22073**		
N/A	17-Oct-2023	4.3	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-DATA-241123/1205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			update, insert or delete access to some of Java VM accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22096**		
N/A	17-Oct-2023	2.4	Vulnerability in the Oracle Database Sharding component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows high privileged attacker having Create Session, Select Any Dictionary privilege with network access via Oracle Net to compromise Oracle Database Sharding. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-DATA-241123/1206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Database Sharding. CVSS 3.1 Base Score 2.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22074**		
N/A	17-Oct-2023	2.4	Vulnerability in the Oracle Database Sharding component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows high privileged attacker having Create Session, Create Any View, Select Any Table privilege with network access via Oracle Net to compromise Oracle Database Sharding. Successful attacks require human interaction from a person other than	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-DATA-241123/1207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Database Sharding. CVSS 3.1 Base Score 2.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22075**		
Product: e-business_suite					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12					
N/A	17-Oct-2023	6.5	Vulnerability in the Oracle iRecruitment product of Oracle E-Business Suite (component: Requisition and Vacancy). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iRecruitment. Successful attacks	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-E-BU-241123/1208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle iRecruitment accessible data as well as unauthorized read access to a subset of Oracle iRecruitment accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-22093**		
N/A	17-Oct-2023	6.1	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Personalization). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-E-BU-241123/1209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Applications Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data as well as unauthorized read access to a subset of Oracle Applications Framework accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22076**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: enterprise_command_center_framework					
Affected Version(s): 10.0					
N/A	17-Oct-2023	6.5	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: API). Supported versions that are affected are ECC: 8, 9 and 10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Command Center Framework. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Command Center Framework accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-ENTE-241123/1210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22106		
N/A	17-Oct-2023	6.1	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: UI Components). Supported versions that are affected are ECC: 8, 9 and 10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Command Center Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Command Center Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-ENTE-241123/1211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			delete access to some of Oracle Enterprise Command Center Framework accessible data as well as unauthorized read access to a subset of Oracle Enterprise Command Center Framework accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22107**		
Affected Version(s): 8.0					
N/A	17-Oct-2023	6.5	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: API). Supported versions that are affected are ECC: 8, 9 and 10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-ENTE-241123/1212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle Enterprise Command Center Framework. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Command Center Framework accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22106**		
N/A	17-Oct-2023	6.1	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: UI Components). Supported versions that are affected are ECC: 8, 9 and 10. Easily exploitable vulnerability allows unauthenticated attacker with network access via	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-ENTE-241123/1213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP to compromise Oracle Enterprise Command Center Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Command Center Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Enterprise Command Center Framework accessible data as well as unauthorized read access to a subset of Oracle Enterprise Command Center Framework accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22107**		
Affected Version(s): 9.0					
N/A	17-Oct-2023	6.5	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: API). Supported versions that are affected are ECC: 8, 9 and 10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Command Center Framework. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Command Center Framework accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-ENTE-241123/1214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22106**		
N/A	17-Oct-2023	6.1	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: UI Components). Supported versions that are affected are ECC: 8, 9 and 10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Command Center Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Command Center Framework, attacks may significantly impact additional products (scope change). Successful attacks	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-ENTE-241123/1215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Enterprise Command Center Framework accessible data as well as unauthorized read access to a subset of Oracle Enterprise Command Center Framework accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22107**		
Product: enterprise_session_border_controller					
Affected Version(s): From (including) 9.0 Up to (including) 9.2					
N/A	17-Oct-2023	4.3	Vulnerability in the Oracle Enterprise Session Border Controller product of Oracle Communications (component: Web UI). Supported versions that are affected are 9.0-9.2. Easily exploitable	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-ENTE-241123/1216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Enterprise Session Border Controller. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Enterprise Session Border Controller accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22083**		
Product: flexcube_universal_banking					
Affected Version(s): 12.3.0					
N/A	17-Oct-2023	6.5	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure).	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-FLEX-241123/1217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and 14.5-14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Universal Banking, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.1 Base Score 6.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L). **CVE ID : CVE-2023-22118**		
N/A	17-Oct-2023	5.9	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and 14.5-14.7. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-FLEX-241123/1218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:L). **CVE ID : CVE-2023-22119**		
N/A	17-Oct-2023	5.4	Vulnerability in the Oracle FLEXCUBE Universal Banking	https://www.oracle.com/security-	A-ORA-FLEX-241123/1219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and 14.5-14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Universal Banking, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read	alerts/cpuoct2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to a subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22117**		
Affected Version(s): 12.4.0					
N/A	17-Oct-2023	6.5	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and 14.5-14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-FLEX-241123/1220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker and while the vulnerability is in Oracle FLEXCUBE Universal Banking, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.1 Base Score 6.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22118		
N/A	17-Oct-2023	5.9	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and 14.5-14.7. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized update, insert or delete access to some of Oracle	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-FLEX-241123/1221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FLEXCUBE Universal Banking accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:L). **CVE ID : CVE-2023-22119**		
N/A	17-Oct-2023	5.4	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and 14.5-14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-FLEX-241123/1222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Universal Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Universal Banking, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22117**		
Affected Version(s): From (including) 14.0.0 Up to (including) 14.3.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Oct-2023	6.5	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and 14.5-14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Universal Banking, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-FLEX-241123/1223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.1 Base Score 6.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L). **CVE ID : CVE-2023-22118**		
N/A	17-Oct-2023	5.9	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and 14.5-14.7. Difficult to exploit vulnerability allows low	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-FLEX-241123/1224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/A		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			C:H/PR:L/UI:R/S:U/C:H/I:L/A:L). **CVE ID : CVE-2023-22119**		
N/A	17-Oct-2023	5.4	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and 14.5-14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Universal Banking, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-FLEX-241123/1225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22117**		
Affected Version(s): From (including) 14.5.0 Up to (including) 14.7.0					
N/A	17-Oct-2023	6.5	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and 14.5-14.7. Easily exploitable vulnerability allows low privileged attacker with network	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-FLEX-241123/1226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Universal Banking, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.1 Base Score 6.5 (Confidentiality,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L). **CVE ID : CVE-2023-22118**		
N/A	17-Oct-2023	5.9	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and 14.5-14.7. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-FLEX-241123/1227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FLEXCUBE Universal Banking accessible data as well as unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:L). **CVE ID : CVE-2023-22119**		
N/A	17-Oct-2023	5.4	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.3, 12.4, 14.0-14.3 and 14.5-14.7. Easily	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-FLEX-241123/1228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Universal Banking, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22117**		
Product: graalvm_for_jdk					
Affected Version(s): 21					
N/A	17-Oct-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u381, 8u381-perf, 11.0.20, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 20.3.11, 21.3.7 and 22.3.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-GRAA-241123/1229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22081		
N/A	17-Oct-2023	4.8	Vulnerability in the Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 20.3.11, 21.3.7 and 22.3.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-GRAA-241123/1230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to a subset of Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-22091**		
N/A	17-Oct-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u381-perf, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 21.3.7 and 22.3.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-GRAA-241123/1231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition,. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22025**		
Affected Version(s): 17.0.8					
N/A	17-Oct-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u381, 8u381-perf, 11.0.20, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 20.3.11, 21.3.7 and 22.3.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-GRAA-241123/1232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22081		
N/A	17-Oct-2023	4.8	Vulnerability in the Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 20.3.11, 21.3.7 and 22.3.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-GRAA-241123/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to a subset of Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-22091**		
N/A	17-Oct-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u381-perf, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 21.3.7 and 22.3.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-GRAA-241123/1234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition,. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22025**		
Product: hospitality_opera_5_property_services					
Affected Version(s): 5.6					
N/A	17-Oct-2023	8.8	Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-HOSP-241123/1235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-22085**		
N/A	17-Oct-2023	8.8	Vulnerability in the Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in takeover of Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-HOSP-241123/1236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22087		
Product: http_server					
Affected Version(s): 12.2.1.4.0					
N/A	17-Oct-2023	7.5	Vulnerability in the Oracle HTTP Server product of Oracle Fusion Middleware (component: Web Listener). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle HTTP Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22019**	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-HTTP-241123/1237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: jdk					
Affected Version(s): 17.0.8					
N/A	17-Oct-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u381, 8u381-perf, 11.0.20, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 20.3.11, 21.3.7 and 22.3.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-JDK-241123/1238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22081**		
N/A	17-Oct-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle	https://www.oracle.com/security-	A-ORA-JDK-241123/1239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition, product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u381-perf, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 21.3.7 and 22.3.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition,. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, accessible data. Note: This vulnerability can be exploited by using APIs in the	alerts/cpuoct2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22025**		
Affected Version(s): 1.8.0					
N/A	17-Oct-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: CORBA). Supported versions that are affected are Oracle Java SE: 8u381, 8u381-perf;	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-JDK-241123/1240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle GraalVM Enterprise Edition: 20.3.11 and 21.3.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via CORBA to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/A		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			C:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22067**		
N/A	17-Oct-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u381, 8u381-perf, 11.0.20, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 20.3.11, 21.3.7 and 22.3.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-JDK-241123/1241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22081**		
N/A	17-Oct-2023	3.7	Vulnerability in the Oracle Java SE,	https://www.oracle.com/securi	A-ORA-JDK-241123/1242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u381-perf, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 21.3.7 and 22.3.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition,. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, accessible data. Note: This vulnerability can	ty-alerts/cpuoct2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22025**		
Affected Version(s): 11.0.2					
N/A	17-Oct-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-JDK-241123/1243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are affected are Oracle Java SE: 8u381, 8u381-perf, 11.0.20, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 20.3.11, 21.3.7 and 22.3.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22081**		
Affected Version(s): 21.0.0					
N/A	17-Oct-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u381, 8u381-perf, 11.0.20, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21;	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-JDK-241123/1244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle GraalVM Enterprise Edition: 20.3.11, 21.3.7 and 22.3.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22081**		
N/A	17-Oct-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u381-perf, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 21.3.7 and 22.3.3. Difficult to exploit vulnerability allows unauthenticated	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-JDK-241123/1245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition,. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22025**		
Product: jre					
Affected Version(s): 17.0.8					
N/A	17-Oct-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u381, 8u381-perf, 11.0.20, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 20.3.11, 21.3.7 and 22.3.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM for JDK,	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-JRE-241123/1246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22081**		
N/A	17-Oct-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u381-perf, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 21.3.7 and 22.3.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition,. Successful attacks of this vulnerability can result in unauthorized update, insert or	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-JRE-241123/1247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22025**		
Affected Version(s): 1.8.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Oct-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: CORBA). Supported versions that are affected are Oracle Java SE: 8u381, 8u381-perf; Oracle GraalVM Enterprise Edition: 20.3.11 and 21.3.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via CORBA to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-JRE-241123/1248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22067**		
N/A	17-Oct-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u381, 8u381-perf, 11.0.20, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 20.3.11, 21.3.7 and 22.3.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-JRE-241123/1249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22081**		
N/A	17-Oct-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u381-perf, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 21.3.7 and 22.3.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition,. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-JRE-241123/1250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22025**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 11.0.2					
N/A	17-Oct-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u381, 8u381-perf, 11.0.20, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 20.3.11, 21.3.7 and 22.3.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-JRE-241123/1251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22081**		
Affected Version(s): 21.0.0					
N/A	17-Oct-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-JRE-241123/1252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u381, 8u381-perf, 11.0.20, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 20.3.11, 21.3.7 and 22.3.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22081**		
N/A	17-Oct-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, product of Oracle Java SE (component: Hotspot). Supported versions that are affected	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-JRE-241123/1253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are Oracle Java SE: 8u381-perf, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 21.3.7 and 22.3.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition,. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22025**		
Product: mysql					
Affected Version(s): 8.1.0					
N/A	17-Oct-2023	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server.	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22059**		
N/A	17-Oct-2023	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). The supported version that is affected is 8.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22095**		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22032**		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/A	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			C:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22066**		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22068**	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22070**	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1259
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component:	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22078**		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.43 and prior, 8.0.34 and	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22084**		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22097**		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server.	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22103**		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22114**		
Affected Version(s): From (including) 5.0.0 Up to (including) 5.7.42					
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.42 and prior and 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22015**		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.42 and prior and 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22026**		
Affected Version(s): From (including) 5.0.0 Up to (including) 5.7.43					
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.43 and prior and 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/A	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			C:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22028**		
Affected Version(s): From (including) 5.7.0 Up to (including) 5.7.43					
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.43 and prior, 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22084		
Affected Version(s): From (including) 8.0 Up to (including) 8.0.31					
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.42 and prior and 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22015**	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.42 and prior and 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22026**	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1270
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL	https://www.oracle.com/security-	A-ORA-MYSQ-241123/1271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(component: Server: Optimizer). Supported versions that are affected are 5.7.43 and prior and 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22028**	alerts/cpuoct2023.html	
Affected Version(s): From (including) 8.0 Up to (including) 8.0.33					
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22065**		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22110**		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: UDF). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22111**		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22115**		
N/A	17-Oct-2023	2.7	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data.	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22113**		
Affected Version(s): From (including) 8.0 Up to (including) 8.0.34					
N/A	17-Oct-2023	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22059**		
N/A	17-Oct-2023	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22079		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22032**	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1279
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle	https://www.oracle.com/security-	A-ORA-MYSQ-241123/1280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22064**	alerts/cpuoct2023.html	
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22066**		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22068**		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22070**		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22078**		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.43 and prior, 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22084**		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22092**		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22097		
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22103**	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1288
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle	https://www.oracle.com/security-	A-ORA-MYSQ-241123/1289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22112**	alerts/cpuoct2023.html	
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are 8.0.34 and prior and 8.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22114**		
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.32					
N/A	17-Oct-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22104**		
Product: mysql_connector\/j					
Affected Version(s): * Up to (including) 8.1.0					
N/A	17-Oct-2023	8.3	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.1.0 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			multiple protocols to compromise MySQL Connectors. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Connectors, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2023-22102**		
Product: mysql_installer					
Affected Version(s): * Up to (excluding) 1.6.8					
N/A	17-Oct-2023	7.9	Vulnerability in the MySQL Installer product of Oracle MySQL (component: Installer: General). Supported versions that are affected are Prior to 1.6.8. Easily exploitable	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-MYSQ-241123/1293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Installer executes to compromise MySQL Installer. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Installer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Installer accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Installer. Note: This patch is used in MySQL Server bundled version 8.0.35 and 5.7.44. CVSS 3.1 Base Score 7.9 (Integrity and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:N/I:H/A:H). **CVE ID : CVE-2023-22094**		
Product: outside_in_technology					
Affected Version(s): 8.5.6					
N/A	17-Oct-2023	6.3	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Content Access SDK, Image Export SDK, PDF Export SDK, HTML Export SDK). The supported version that is affected is 8.5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-OUTS-241123/1294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2023-22127**		
Product: peoplesoft_enterprise_cost_center_common_application_objects					
Affected Version(s): 9.2					
N/A	17-Oct-2023	6.5	Vulnerability in the PeopleSoft Enterprise CC Common Application Objects product of Oracle PeopleSoft (component: Events & Notifications). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-PEOP-241123/1295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with network access via HTTP to compromise PeopleSoft Enterprise CC Common Application Objects. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise CC Common Application Objects accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22090**		
Product: peoplesoft_enterprise_peopletools					
Affected Version(s): 8.59					
N/A	17-Oct-2023	6.1	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). Supported versions that are affected are 8.59 and 8.60.	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-PEOP-241123/1296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22080**		
Affected Version(s): 8.60					
N/A	17-Oct-2023	6.1	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). Supported versions that are affected are 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-PEOP-241123/1297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22080**		
Product: sun_zfs_storage_appliance_kit					
Affected Version(s): 8.8.60					
N/A	17-Oct-2023	5.9	Vulnerability in the Sun ZFS Storage Appliance product of Oracle Systems (component: Core). The supported version that is affected is 8.8.60. Difficult to exploit vulnerability	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-SUN_-241123/1298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated attacker with network access via HTTP to compromise Sun ZFS Storage Appliance. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Sun ZFS Storage Appliance. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22130**		
Product: vm_virtualbox					
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.12					
N/A	17-Oct-2023	8.2	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.12. Easily exploitable vulnerability allows high privileged attacker with logon to the	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-VM_V-241123/1299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. Note: Only applicable to 7.0.x platform. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2023-22099**		
N/A	17-Oct-2023	7.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.12. Easily exploitable	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-VM_V-241123/1300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Only applicable to 7.0.x platform. CVSS 3.1 Base Score 7.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			:L/PR:H/UI:N/S:C/C:H/I:N/A:H). **CVE ID : CVE-2023-22100**		
N/A	17-Oct-2023	7.3	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.12. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox as well as unauthorized	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-VM_V-241123/1301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			update, insert or delete access to some of Oracle VM VirtualBox accessible data and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. Note: Only applicable to 7.0.x platform. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H). **CVE ID : CVE-2023-22098**		
Product: webcenter_content					
Affected Version(s): 12.2.1.4.0					
N/A	17-Oct-2023	5.3	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-WEBC-241123/1302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22126**		
Product: weblogic_server					
Affected Version(s): 12.2.1.4.0					
N/A	17-Oct-2023	9.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server.	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-WEBL-241123/1303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-22069**		
N/A	17-Oct-2023	9.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-WEBL-241123/1304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-22089**		
N/A	17-Oct-2023	8.1	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/A	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-WEBL-241123/1305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			C:H/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-22101**		
N/A	17-Oct-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22086**	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-WEBL-241123/1306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Oct-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22108**	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-WEBL-241123/1307
Affected Version(s): 12.2.1.3.0					
N/A	17-Oct-2023	9.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion	https://www.oracle.com/security-	A-ORA-WEBL-241123/1308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Middleware (component: Core). The supported version that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-22072**	alerts/cpuoct2023.html	
Affected Version(s): 14.1.1.0.0					
N/A	17-Oct-2023	9.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-WEBL-241123/1309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-22069**		
N/A	17-Oct-2023	9.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-WEBL-241123/1310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-22089**		
N/A	17-Oct-2023	8.1	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-WEBL-241123/1311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-22101**		
N/A	17-Oct-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-WEBL-241123/1312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22086**		
N/A	17-Oct-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	https://www.oracle.com/security-alerts/cpuoct2023.html	A-ORA-WEBL-241123/1313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22108		
Vendor: order_auto_complete_for_woocommerce_project					
Product: order_auto_complete_for_woocommerce					
Affected Version(s): * Up to (including) 1.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Kardi Order auto complete for WooCommerce plugin <= 1.2.0 versions. **CVE ID : CVE-2023-45072**	N/A	A-ORD-ORDE-241123/1314
Vendor: oretnom23					
Product: packers_and_movers_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	9.8	Sourcecodester Packers and Movers Management System v1.0 is vulnerable to SQL Injection via mpms/?p=services/view_service&id. **CVE ID : CVE-2023-46435**	N/A	A-ORE-PACK-241123/1315
Vendor: osgeo					
Product: geoserver					
Affected Version(s): * Up to (excluding) 2.22.5					
Server-Side Request Forgery (SSRF)	25-Oct-2023	9.8	GeoServer is an open source software server written in Java that allows users to share and edit	https://github.com/geoserver/geoserver/security/advisories/GHSA-5pr3-m5hm-9956	A-OSG-GEOS-241123/1316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			geospatial data. The OGC Web Processing Service (WPS) specification is designed to process information from any server using GET and POST requests. This presents the opportunity for Server Side Request Forgery. This vulnerability has been patched in version 2.22.5 and 2.23.2. **CVE ID : CVE-2023-43795**		
Server-Side Request Forgery (SSRF)	25-Oct-2023	5.3	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. The WMS specification defines an ``sld=<url>`` parameter for GetMap, GetLegendGraphic and GetFeatureInfo operations for user supplied "dynamic styling". Enabling the use of dynamic styles, without also configuring URL checks, provides the opportunity for	https://github.com/geoserver/geoserver/security/advisories/GHSA-cqpc-x2c6-2gmf	A-OSG-GEOS-241123/1317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service Side Request Forgery. This vulnerability can be used to steal user NetNTLMv2 hashes which could be relayed or cracked externally to gain further access. This vulnerability has been patched in versions 2.22.5 and 2.23.2. **CVE ID : CVE-2023-41339**		
Affected Version(s): From (including) 2.23.0 Up to (excluding) 2.23.2					
Server-Side Request Forgery (SSRF)	25-Oct-2023	9.8	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. The OGC Web Processing Service (WPS) specification is designed to process information from any server using GET and POST requests. This presents the opportunity for Server Side Request Forgery. This vulnerability has been patched in version 2.22.5 and 2.23.2.	https://github.com/geoserver/geoserver/security/advisories/GHSA-5pr3-m5hm-9956	A-OSG-GEOS-241123/1318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43795		
Server-Side Request Forgery (SSRF)	25-Oct-2023	5.3	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. The WMS specification defines an ``sld=<url>`` parameter for GetMap, GetLegendGraphic and GetFeatureInfo operations for user supplied "dynamic styling". Enabling the use of dynamic styles, without also configuring URL checks, provides the opportunity for Service Side Request Forgery. This vulnerability can be used to steal user NetNTLMv2 hashes which could be relayed or cracked externally to gain further access. This vulnerability has been patched in versions 2.22.5 and 2.23.2. **CVE ID : CVE-2023-41339**	https://github.com/geoserver/geoserver/security/advisories/GHSA-cqpc-x2c6-2gmf	A-OSG-GEOS-241123/1319
Vendor: osmansorkar					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ajax_archive_calendar					
Affected Version(s): * Up to (excluding) 2.6.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Osmansorkar Ajax Archive Calendar plugin <= 2.6.7 versions. **CVE ID : CVE-2023-46069**	N/A	A-OSM-AJAX-241123/1320
Vendor: Otrs					
Product: otrs					
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.34					
Improper Certificate Validation	16-Oct-2023	9.1	The functions to fetch e-mail via POP3 or IMAP as well as sending e-mail via SMTP use OpenSSL for static SSL or TLS based communication. As the SSL_get_verify_result() function is not used the certificated is trusted always and it can not be ensured that the certificate satisfies all necessary security requirements. This could allow an attacker to use an invalid certificate	https://otrs.com/release-notes/otrs-security-advisory-2023-10/	A-OTR-OTRS-241123/1321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to claim to be a trusted host, use expired certificates, or conduct other attacks that could be detected if the certificate is properly validated. This issue affects OTRS: from 7.0.X before 7.0.47, from 8.0.X before 8.0.37; ((OTRS)) Community Edition: from 6.0.X through 6.0.34. **CVE ID : CVE-2023-5422**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-2023	5.5	An attacker who is logged into OTRS as an user with privileges to create and change customer user data may manipulate the CustomerID field to execute JavaScript code that runs immediatly after the data is saved.The issue onlyoccurs if the configuration for AdminCustomerUser::UseAutoComple	https://otrs.com/release-notes/otrs-security-advisory-2023-09/	A-OTR-OTRS-241123/1322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			te was changed before. This issue affects OTRS: from 7.0.X before 7.0.47, from 8.0.X before 8.0.37; ((OTRS)) Community Edition: from 6.0.X through 6.0.34. **CVE ID : CVE-2023-5421**		
N/A	16-Oct-2023	5.3	The loading of external images is not blocked, even if configured, if the attacker uses protocol-relative URL in the payload. This can be used to retreive the IP of the user.This issue affects OTRS: from 7.0.X before 7.0.47, from 8.0.X before 8.0.37; ((OTRS)) Community Edition: from 6.0.X through 6.0.34. **CVE ID : CVE-2023-38059**	https://otrs.com/release-notes/otrs-security-advisory-2023-08/	A-OTR-OTRS-241123/1323
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.47					
Improper Certificate Validation	16-Oct-2023	9.1	The functions to fetch e-mail via POP3 or IMAP as well as sending e-mail via SMTP use	https://otrs.com/release-notes/otrs-security-	A-OTR-OTRS-241123/1324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OpenSSL for static SSL or TLS based communication. As the SSL_get_verify_result() function is not used the certificated is trusted always and it can not be ensured that the certificate satisfies all necessary security requirements. This could allow an attacker to use an invalid certificate to claim to be a trusted host, use expired certificates, or conduct other attacks that could be detected if the certificate is properly validated. This issue affects OTRS: from 7.0.X before 7.0.47, from 8.0.X before 8.0.37; ((OTRS)) Community Edition: from 6.0.X through 6.0.34.	advisory-2023-10/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5422		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-2023	5.5	An attacker who is logged into OTRS as an user with privileges to create and change customer user data may manipulate the CustomerID field to execute JavaScript code that runs immediatly after the data is saved.The issue onlyoccurs if the configuration for AdminCustomerUser::UseAutoComplete was changed before. This issue affects OTRS: from 7.0.X before 7.0.47, from 8.0.X before 8.0.37; ((OTRS)) Community Edition: from 6.0.X through 6.0.34. **CVE ID : CVE-2023-5421**	https://otrs.com/release-notes/otrs-security-advisory-2023-09/	A-OTR-OTRS-241123/1325
N/A	16-Oct-2023	5.3	The loading of external images is not blocked, even if configured, if the attacker uses protocol-relative URL in the payload. This can be used to	https://otrs.com/release-notes/otrs-security-advisory-2023-08/	A-OTR-OTRS-241123/1326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retreive the IP of the user.This issue affects OTRS: from 7.0.X before 7.0.47, from 8.0.X before 8.0.37; ((OTRS)) Community Edition: from 6.0.X through 6.0.34. **CVE ID : CVE-2023-38059**		
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.0.37					
Improper Certificate Validation	16-Oct-2023	9.1	The functions to fetch e-mail via POP3 or IMAP as well as sending e-mail via SMTP use OpenSSL for static SSL or TLS based communication. As the SSL_get_verify_result() function is not used the certificated is trusted always and it can not be ensured that the certificate satisfies all necessary security requirements. This could allow an attacker to use an invalid certificate to claim to be a trusted host,	https://otrs.com/release-notes/otrs-security-advisory-2023-10/	A-OTR-OTRS-241123/1327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use expired certificates, or conduct other attacks that could be detected if the certificate is properly validated. This issue affects OTRS: from 7.0.X before 7.0.47, from 8.0.X before 8.0.37; ((OTRS)) Community Edition: from 6.0.X through 6.0.34. **CVE ID : CVE-2023-5422**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-2023	5.5	An attacker who is logged into OTRS as an user with privileges to create and change customer user data may manipulate the CustomerID field to execute JavaScript code that runs immediatly after the data is saved.The issue onlyoccurs if the configuration for AdminCustomerUser::UseAutoComplete was changed before.	https://otrs.com/release-notes/otrs-security-advisory-2023-09/	A-OTR-OTRS-241123/1328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects OTRS: from 7.0.X before 7.0.47, from 8.0.X before 8.0.37; ((OTRS)) Community Edition: from 6.0.X through 6.0.34. **CVE ID : CVE-2023-5421**		
N/A	16-Oct-2023	5.3	The loading of external images is not blocked, even if configured, if the attacker uses protocol-relative URL in the payload. This can be used to retreive the IP of the user.This issue affects OTRS: from 7.0.X before 7.0.47, from 8.0.X before 8.0.37; ((OTRS)) Community Edition: from 6.0.X through 6.0.34. **CVE ID : CVE-2023-38059**	https://otrs.com/release-notes/otrs-security-advisory-2023-08/	A-OTR-OTRS-241123/1329
Vendor: pagelayer					
Product: pagelayer					
Affected Version(s): * Up to (excluding) 1.7.7					
N/A	16-Oct-2023	6.1	The Page Builder: Pagelayer WordPress plugin before 1.7.7	N/A	A-PAG-PAGE-241123/1330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			doesn't prevent unauthenticated attackers from updating a post's header or footer code on scheduled posts. **CVE ID : CVE-2023-4687**		
Affected Version(s): * Up to (excluding) 1.7.8					
N/A	16-Oct-2023	5.4	The Page Builder: Pagelayer WordPress plugin before 1.7.8 doesn't prevent attackers with author privileges and higher from inserting malicious JavaScript inside a post's header or footer code. **CVE ID : CVE-2023-5087**	N/A	A-PAG-PAGE-241123/1331
Vendor: palantir					
Product: orbital_simulator					
Affected Version(s): * Up to (excluding) 0.692.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Oct-2023	7.5	Gotham Orbital-Simulator service prior to 0.692.0 was found to be vulnerable to a Path traversal issue allowing an unauthenticated user to read arbitrary files on the file system. **CVE ID : CVE-2023-30967**	https://palantir.safebase.us/?tcuUid=8fd5809f-26f8-406e-b36f-4a6596a19d79	A-PAL-ORBI-241123/1332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: tiles					
Affected Version(s): * Up to (excluding) 4.326.0					
Missing Authorization	26-Oct-2023	6.5	The Palantir Tiles1 service was found to be vulnerable to an API wide issue where the service was not performing authentication/authorization on all the endpoints. **CVE ID : CVE-2023-30969**	https://palantir.safebase.us/?tcuUid=afcbc9b2-de62-44b9-b28b-2ebf0684fbf7	A-PAL-TILE-241123/1333
Vendor: palletsprojects					
Product: werkzeug					
Affected Version(s): * Up to (excluding) 3.0.1					
Out-of-bounds Write	25-Oct-2023	7.5	Werkzeug is a comprehensive WSGI web application library. If an upload of a file that starts with CR or LF and then is followed by megabytes of data without these characters: all of these bytes are appended chunk by chunk into internal bytearray and lookup for boundary is performed on growing buffer. This allows an attacker to cause a denial of service by	https://github.com/pallets/werkzeug/commit/f3c803b3ade485a45f12b6d6617595350c0f03e2, https://github.com/pallets/werkzeug/security/advisories/GHSA-hrfv-mqp8-q5rw	A-PAL-WERK-241123/1334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted multipart data to an endpoint that will parse it. The amount of CPU time required can block worker processes from handling legitimate requests. This vulnerability has been patched in version 3.0.1. **CVE ID : CVE-2023-46136**		
Vendor: Papercut					
Product: papercut_mf					
Affected Version(s): * Up to (excluding) 22.1.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Oct-2023	6.5	A Path Traversal vulnerability exists in PaperCut NG before 22.1.1 and PaperCut MF before 22.1.1. Under specific conditions, this could potentially allow an authenticated attacker to achieve read-only access to the server's filesystem, because requests beginning with "GET /ui/static/..//.." reach getStaticContent in UIContentResource.class in the static-content-files servlet.	https://www.papercut.com/kb/Main/SecurityBulletinJune2023, https://www.papercut.com/kb/Main/PO-1216-and-PO-1219#security-notifications	A-PAP-PAPE-241123/1335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31046		
Product: papercut_ng					
Affected Version(s): * Up to (excluding) 22.1.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Oct-2023	6.5	A Path Traversal vulnerability exists in PaperCut NG before 22.1.1 and PaperCut MF before 22.1.1. Under specific conditions, this could potentially allow an authenticated attacker to achieve read-only access to the server's filesystem, because requests beginning with "GET /ui/static/..//.." reach getStaticContent in UIContentResource.class in the static-content-files servlet. **CVE ID : CVE-2023-31046**	https://www.papercut.com/kb/Main/SecurityBulletinJune2023, https://www.papercut.com/kb/Main/PO-1216-and-PO-1219#security-notifications	A-PAP-PAPE-241123/1336
Vendor: parseplatform					
Product: parse-server					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 5.5.6					
Improper Limitation of a Pathname to a Restricted Directory	25-Oct-2023	7.5	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Parse Server crashes when	https://github.com/parse-community/parse-server/security/advisories/GHSA-792q-q67h-w579,	A-PAR-PARS-241123/1337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			uploading a file without extension. This vulnerability has been patched in versions 5.5.6 and 6.3.1. **CVE ID : CVE-2023-46119**	https://github.com/parse-community/parse-server/commit/686a9f282dc23c31beab3d93e6d21ccd0e1328fe	
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.3.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Oct-2023	7.5	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Parse Server crashes when uploading a file without extension. This vulnerability has been patched in versions 5.5.6 and 6.3.1. **CVE ID : CVE-2023-46119**	https://github.com/parse-community/parse-server/security/advisories/GHSA-792q-q67h-w579, https://github.com/parse-community/parse-server/commit/686a9f282dc23c31beab3d93e6d21ccd0e1328fe	A-PAR-PARS-241123/1338
Vendor: paymentsplugin					
Product: wp_full_stripe_free					
Affected Version(s): * Up to (including) 1.6.1					
Improper Neutralization of Input During Web Page Generation	26-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Mammothology WP Full Stripe Free plugin <= 1.6.1 versions.	N/A	A-PAY-WP_F-241123/1339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-46088**		
Vendor: pega					
Product: platform					
Affected Version(s): From (including) 8.1.0 Up to (excluding) 8.7.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	6.1	Pega Platform versions 8.1 to Infinity 23.1.0 are affected by an XSS issue with task creation **CVE ID : CVE-2023-32087**	https://support.pega.com/support-doc/pega-security-advisory-e23-vulnerability-remediation-note	A-PEG-PLAT-241123/1340
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	6.1	Pega Platform versions 8.1 to Infinity 23.1.0 are affected by an XSS issue with ad-hoc case creation **CVE ID : CVE-2023-32088**	https://support.pega.com/support-doc/pega-security-advisory-e23-vulnerability-remediation-note	A-PEG-PLAT-241123/1341
Affected Version(s): From (including) 8.1.0 Up to (including) 8.8.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	6.1	Pega Platform versions 8.1 to 8.8.2 are affected by an XSS issue with Pin description **CVE ID : CVE-2023-32089**	https://support.pega.com/support-doc/pega-security-advisory-e23-vulnerability-remediation-note	A-PEG-PLAT-241123/1342
Affected Version(s): From (including) 8.8.0 Up to (excluding) 8.8.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	6.1	Pega Platform versions 8.1 to Infinity 23.1.0 are affected by an XSS issue with task creation **CVE ID : CVE-2023-32087**	https://support.pega.com/support-doc/pega-security-advisory-e23-vulnerability-remediation-note	A-PEG-PLAT-241123/1343
Improper Neutralization of Input During Web Page Generation	18-Oct-2023	6.1	Pega Platform versions 8.1 to Infinity 23.1.0 are affected by an XSS	https://support.pega.com/support-doc/pega-security-advisory-e23-vulnerability-	A-PEG-PLAT-241123/1344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			issue with ad-hoc case creation **CVE ID : CVE-2023-32088**	remediation-note	
Vendor: peppermint					
Product: peppermint					
Affected Version(s): * Up to (excluding) 0.2.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	30-Oct-2023	7.5	Peppermint Ticket Management before 0.2.4 allows remote attackers to read arbitrary files via a /api/v1/users/file/download?filepath=./../ POST request. **CVE ID : CVE-2023-46863**	https://github.com/Peppermint-Lab/peppermint/issues/108	A-PEP-PEPP-241123/1345
Affected Version(s): * Up to (including) 0.2.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	30-Oct-2023	5.3	Peppermint Ticket Management through 0.2.4 allows remote attackers to read arbitrary files via a /api/v1/ticket/1/file/download?filepath=../ POST request. **CVE ID : CVE-2023-46864**	https://github.com/Peppermint-Lab/peppermint/issues/171	A-PEP-PEPP-241123/1346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: peterkeung					
Product: peter\'s_custom_anti-spam					
Affected Version(s): * Up to (including) 3.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Peter Keung Peter's Custom Anti-Spam plugin <= 3.2.2 versions. **CVE ID : CVE-2023-45759**	N/A	A-PET-PETE-241123/1347
Vendor: Pfsense					
Product: pfsense					
Affected Version(s): 2.6.0					
Allocation of Resources Without Limits or Throttling	25-Oct-2023	4.9	Pfsense CE version 2.6.0 is vulnerable to No rate limit which can lead to an attacker creating multiple malicious users in firewall. **CVE ID : CVE-2023-29973**	N/A	A-PFS-PFSE-241123/1348
Vendor: phpdeveloper					
Product: sort_searchresult_by_title					
Affected Version(s): * Up to (including) 10.0					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Codex-m Sort SearchResult By Title plugin <= 10.0 versions. **CVE ID : CVE-2023-45639**	N/A	A-PHP-SORT-241123/1349
Vendor: phpgurukul					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nipah_virus_testing_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	9.8	SQL Injection vulnerability in PHPGurukul Nipah virus (NiV) " Testing Management System v.1.0 allows a remote attacker to escalate privileges via a crafted request to the new-user-testing.php endpoint. **CVE ID : CVE-2023-46584**	N/A	A-PHP-NIPA-241123/1350
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	9.8	A vulnerability was found in PHPGurukul Nipah Virus Testing Management System 1.0 and classified as critical. This issue affects some unknown processing of the file login.php. The manipulation of the argument username leads to sql injection. The attack may be initiated remotely. The identifier VDB-243617 was assigned to this vulnerability. **CVE ID : CVE-2023-5804**	N/A	A-PHP-NIPA-241123/1351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	6.1	Cross-Site Scripting (XSS) vulnerability in PHPGurukul Nipah virus (NiV) " Testing Management System v.1.0 allows attackers to execute arbitrary code via a crafted payload injected into the State field. **CVE ID : CVE-2023-46583**	N/A	A-PHP-NIPA-241123/1352
Product: online_railway_catering_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	9.8	A vulnerability was found in PHPGurukul Online Railway Catering System 1.0. It has been classified as critical. Affected is an unknown function of the file index.php of the component Login. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-243600. **CVE ID : CVE-2023-5794**	N/A	A-PHP-ONLI-241123/1353
Vendor: Phpmyfaq					
Product: phpmyfaq					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 3.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Oct-2023	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.2.1. **CVE ID : CVE-2023-5864**	https://github.com/thorsten/phpmyfaq/commit/b3e5a053b59dcc072d76a55d6ce0311ea30174fa, https://huntr.com/bounties/e4b0e8f4-5e06-49d1-832f-5756573623ad	A-PHP-PHPM-241123/1354
Affected Version(s): * Up to (excluding) 3.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Oct-2023	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository thorsten/phpmyfaq prior to 3.2.2. **CVE ID : CVE-2023-5863**	https://huntr.com/bounties/fbfd4e84-61fb-4063-8f11-15877b8c1f6f, https://github.com/thorsten/phpmyfaq/commit/97e813dcd2022bd10a8770569a8b02591716365f	A-PHP-PHPM-241123/1355
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Oct-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.2.2. **CVE ID : CVE-2023-5867**	https://huntr.com/bounties/5c09b32e-a041-4a1e-a277-eb3e80967df0, https://github.com/thorsten/phpmyfaq/commit/5310cb8c37dc3a5c5aead0898690b14705c433d3	A-PHP-PHPM-241123/1356
Vendor: Pimcore					
Product: pimcore					
Affected Version(s): * Up to (excluding) 11.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Oct-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 11.1.0. **CVE ID : CVE-2023-5873**	https://huntr.com/bounties/701cfc30-22a1-4c4b-9b2f-885c77c290ce, https://github.com/pimcore/pimcore/commit/757375677dc83a44c6c22f26d97452cc5cda5d7c	A-PIM-PIMC-241123/1357
Vendor: Pingidentity					
Product: pingfederate					
Affected Version(s): * Up to (including) 11.3.0					
N/A	25-Oct-2023	4.3	When an AWS DynamoDB table is used for user attribute storage, it is possible to retrieve the attributes of another user using a maliciously crafted request **CVE ID : CVE-2023-34085**	N/A	A-PIN-PING-241123/1358
Affected Version(s): 11.3					
Improper Authentication	25-Oct-2023	9.8	Under a very specific and highly unrecommended configuration, authentication bypass is possible in the PingFederate Identifier First Adapter	N/A	A-PIN-PING-241123/1359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37283		
Uncontrolled Resource Consumption	25-Oct-2023	7.5	PingFederate Administrative Console dependency contains a weakness where console becomes unresponsive with crafted Java class loading enumeration requests **CVE ID : CVE-2023-39219**	N/A	A-PIN-PING-241123/1360
Affected Version(s): From (including) 10.3.0 Up to (including) 10.3.12					
Improper Authentication	25-Oct-2023	9.8	Under a very specific and highly unrecommended configuration, authentication bypass is possible in the PingFederate Identifier First Adapter **CVE ID : CVE-2023-37283**	N/A	A-PIN-PING-241123/1361
Uncontrolled Resource Consumption	25-Oct-2023	7.5	PingFederate Administrative Console dependency contains a weakness where console becomes unresponsive with crafted Java class loading	N/A	A-PIN-PING-241123/1362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enumeration requests **CVE ID : CVE-2023-39219**		
Affected Version(s): From (including) 11.1.0 Up to (including) 11.1.7					
Improper Authentication	25-Oct-2023	9.8	Under a very specific and highly unrecommended configuration, authentication bypass is possible in the PingFederate Identifier First Adapter **CVE ID : CVE-2023-37283**	N/A	A-PIN-PING-241123/1363
Uncontrolled Resource Consumption	25-Oct-2023	7.5	PingFederate Administrative Console dependency contains a weakness where console becomes unresponsive with crafted Java class loading enumeration requests **CVE ID : CVE-2023-39219**	N/A	A-PIN-PING-241123/1364
Affected Version(s): From (including) 11.2.0 Up to (including) 11.2.6					
Improper Authentication	25-Oct-2023	9.8	Under a very specific and highly unrecommended configuration, authentication bypass is possible	N/A	A-PIN-PING-241123/1365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the PingFederate Identifier First Adapter **CVE ID : CVE-2023-37283**		
Uncontrolled Resource Consumption	25-Oct-2023	7.5	PingFederate Administrative Console dependency contains a weakness where console becomes unresponsive with crafted Java class loading enumeration requests **CVE ID : CVE-2023-39219**	N/A	A-PIN-PING-241123/1366
Product: pingid_radius_pcv					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.3					
Missing Authentication for Critical Function	25-Oct-2023	9.8	A first-factor authentication bypass vulnerability exists in the PingFederate with PingID Radius PCV when a MSCHAP authentication request is sent via a maliciously crafted RADIUS client request. **CVE ID : CVE-2023-39930**	N/A	A-PIN-PING-241123/1367
Product: pingone_mfa_integration_kit					
Affected Version(s): 2.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	25-Oct-2023	6.5	PingFederate using the PingOne MFA adapter allows a new MFA device to be paired without requiring second factor authentication from an existing registered device. A threat actor may be able to exploit this vulnerability to register their own MFA device if they have knowledge of a victim user's first factor credentials. **CVE ID : CVE-2023-39231**	N/A	A-PIN-PING-241123/1368
Vendor: pixelative					
Product: google_amp					
Affected Version(s): * Up to (including) 1.5.15					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Pixelative, Mohsin Rafique AMP WP – Google AMP For WordPress plugin <= 1.5.15 versions. **CVE ID : CVE-2023-45831**	N/A	A-PIX-GOOG-241123/1369
Vendor: pixelgrade					
Product: comments_rating					
Affected Version(s): * Up to (including) 1.1.7					
Cross-Site Request	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Pixelgrade	N/A	A-PIX-COMM-241123/1370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Comments Ratings plugin <= 1.1.7 versions. **CVE ID : CVE-2023-45654**		
Product: pixfields					
Affected Version(s): * Up to (including) 0.7.0					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in PixelGrade PixFields plugin <= 0.7.0 versions. **CVE ID : CVE-2023-45655**	N/A	A-PIX-PIXF-241123/1371
Vendor: plugin-planet					
Product: theme_switcha					
Affected Version(s): * Up to (including) 3.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	The Theme Switcha plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'theme_switcha_list' shortcode in all versions up to, and including, 3.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to	https://plugins.trac.wordpress.org/browser/theme-switcha/tags/3.3/inc/plugin-core.php#L445, https://plugins.trac.wordpress.org/changeset/2979783/theme-switcha#file1	A-PLU-THEM-241123/1372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5614**		
Vendor: pluginever					
Product: wc_serial_numbers					
Affected Version(s): * Up to (including) 1.6.3					
Cross-Site Request Forgery (CSRF)	21-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in PluginEver WC Serial Numbers plugin <= 1.6.3 versions. **CVE ID : CVE-2023-46078**	N/A	A-PLU-WC_S-241123/1373
Vendor: pluginus					
Product: bear_-_woocommerce_bulk_editor_and_products_manager_professional					
Affected Version(s): * Up to (including) 1.1.3.3					
Cross-Site Request Forgery (CSRF)	20-Oct-2023	8.8	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the woobe_save_options function. This makes it possible for unauthenticated attackers to modify the plugin's	N/A	A-PLU-BEAR-241123/1374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Additionally, input sanitization and escaping is insufficient resulting in the possibility of malicious script injection. **CVE ID : CVE-2023-4920**		
Cross-Site Request Forgery (CSRF)	20-Oct-2023	4.3	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the woobe_bulkoperations_delete function. This makes it possible for unauthenticated attackers to delete products via a forged request granted they can trick a site administrator into performing an	N/A	A-PLU-BEAR-241123/1375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action such as clicking on a link. **CVE ID : CVE-2023-4923**		
Cross-Site Request Forgery (CSRF)	20-Oct-2023	4.3	The BEAR for WordPress is vulnerable to Missing Authorization in versions up to, and including, 1.1.3.3. This is due to missing capability checks on the woobe_bulkoperations_delete function. This makes it possible for authenticated attackers, with subscriber access or higher, to delete products. **CVE ID : CVE-2023-4924**	N/A	A-PLU-BEAR-241123/1376
Cross-Site Request Forgery (CSRF)	20-Oct-2023	4.3	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the woobe_bulk_delete_products function. This makes it possible for unauthenticated attackers to delete products via a	N/A	A-PLU-BEAR-241123/1377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-4926**		
Cross-Site Request Forgery (CSRF)	20-Oct-2023	4.3	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the create_profile function. This makes it possible for unauthenticated attackers to create profiles via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-4935**	N/A	A-PLU-BEAR-241123/1378
Cross-Site Request Forgery (CSRF)	20-Oct-2023	4.3	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3.	N/A	A-PLU-BEAR-241123/1379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This is due to missing or incorrect nonce validation on the woobe_bulkoperations_apply_default_combination function. This makes it possible for unauthenticated attackers to manipulate products via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-4937**		
Missing Authorization	18-Oct-2023	4.3	The BEAR for WordPress is vulnerable to Missing Authorization in versions up to, and including, 1.1.3.3. This is due to a missing capability check on the woobe_bulkoperations_apply_default_combination function. This makes it possible for authenticated attackers (subscriber or higher) to	N/A	A-PLU-BEAR-241123/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulate products. **CVE ID : CVE-2023-4938**		
Cross-Site Request Forgery (CSRF)	20-Oct-2023	4.3	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the woobe_bulkoperations_swap function. This makes it possible for unauthenticated attackers to manipulate products via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-4940**	N/A	A-PLU-BEAR-241123/1381
Missing Authorization	20-Oct-2023	4.3	The BEAR for WordPress is vulnerable to Missing Authorization in versions up to, and including, 1.1.3.3. This is due to a missing capability check on the woobe_bulkoperati	N/A	A-PLU-BEAR-241123/1382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ons_swap function. This makes it possible for authenticated attackers (subscriber or higher) to manipulate products. **CVE ID : CVE-2023-4941**		
Cross-Site Request Forgery (CSRF)	20-Oct-2023	4.3	The BEAR for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.3.3. This is due to missing or incorrect nonce validation on the woobe_bulkoperations_visibility function. This makes it possible for unauthenticated attackers to manipulate products via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-4942**	N/A	A-PLU-BEAR-241123/1383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	20-Oct-2023	4.3	The BEAR for WordPress is vulnerable to Missing Authorization in versions up to, and including, 1.1.3.3. This is due to a missing capability check on the woobe_bulkoperations_visibility function. This makes it possible for authenticated attackers (subscriber or higher) to manipulate products. **CVE ID : CVE-2023-4943**	N/A	A-PLU-BEAR-241123/1384
Product: wolf_-_wordpress_posts_bulk_editor_and_products_manager_professional					
Affected Version(s): * Up to (excluding) 1.0.7.2					
Cross-Site Request Forgery (CSRF)	25-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in realmag777 WOLF – WordPress Posts Bulk Editor and Manager Professional plugin <= 1.0.7.1 versions. **CVE ID : CVE-2023-46152**	N/A	A-PLU-WOLF-241123/1385
Improper Neutralization of Input During Web Page Generation	17-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in realmag777 WOLF – WordPress Posts Bulk Editor and	N/A	A-PLU-WOLF-241123/1386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Manager Professional plugin <= 1.0.7.1 versions. **CVE ID : CVE-2023-44990**		
Vendor: pogidude					
Product: magic_action_box					
Affected Version(s): * Up to (including) 2.17.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	The Magic Action Box plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 2.17.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5231**	N/A	A-POG-MAGI-241123/1387
Vendor: poptin					
Product: popups					
Affected Version(s): * Up to (excluding) 1.3.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	The Poptin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'poptin-form' shortcode in versions up to, and including, 1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-4961**	https://www.wordfence.com/threat-intel/vulnerabilities/id/778af777-4c98-45cd-9704-1bdc96054aa7?source=cve, https://plugins.trac.wordpress.org/changeset/2968210/poptin#file2	A-POP-POPU-241123/1388
Vendor: posimyth					
Product: nexter_extension					
Affected Version(s): * Up to (including) 2.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in POSIMYTH Nexter Extension plugin <= 2.0.3 versions. **CVE ID : CVE-2023-45750**	N/A	A-POS-NEXT-241123/1389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: posthemes					
Product: posrotatorimg					
Affected Version(s): * Up to (including) 1.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Oct-2023	9.8	In the module "Rotator Img" (posrotatorimg) in versions at least up to 1.1 from PosThemes for PrestaShop, a guest can perform SQL injection. **CVE ID : CVE-2023-45379**	N/A	A-POS-POSR-241123/1390
Vendor: printfriendly					
Product: print\,_pdf\,_email_by_printfriendly					
Affected Version(s): * Up to (including) 5.5.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Print, PDF, Email by PrintFriendly plugin <= 5.5.1 versions. **CVE ID : CVE-2023-25032**	N/A	A-PRI-PRIN-241123/1391
Vendor: prismtechstudios					
Product: modern_footnotes					
Affected Version(s): * Up to (excluding) 1.4.17					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	The Modern Footnotes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode in versions up to, and including,	https://plugins.trac.wordpress.org/changeset/2980695/modern-footnotes, https://www.wordfence.com/threat-intel/vulnerabil	A-PRI-MODE-241123/1392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.4.16 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5618**	ities/id/c20c674f-54b5-470f-b470-07a63501eb4d?source=cve	
Vendor: profosbox					
Product: agp_font_awesome_collection					
Affected Version(s): * Up to (including) 3.2.4					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Alexey Golubnichenko AGP Font Awesome Collection plugin <= 3.2.4 versions. **CVE ID : CVE-2023-45749**	N/A	A-PRO-AGP_-241123/1393
Vendor: projectworlds					
Product: leave_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements	27-Oct-2023	8.8	Leave Management System Project v1.0 is vulnerable to multiple Authenticated SQL	N/A	A-PRO-LEAV-241123/1394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			Injection vulnerabilities. The 'setcasualleave' parameter of the admin/setleaves.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-44480**		
Product: online_art_gallery					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	9.8	Online Art Gallery v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'fnm' parameter of the header.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-43737**	N/A	A-PRO-ONLI-241123/1395
Improper Neutralization of Special Elements used in an SQL	27-Oct-2023	9.8	Online Art Gallery v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'email' parameter	N/A	A-PRO-ONLI-241123/1396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			of the header.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-43738**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Oct-2023	9.8	Online Art Gallery v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'contact' parameter of the header.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-44162**	N/A	A-PRO-ONLI-241123/1397
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	9.8	Online Art Gallery v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'lnm' parameter of the header.php resource does not validate the characters received and they are sent	N/A	A-PRO-ONLI-241123/1398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unfiltered to the database. **CVE ID : CVE-2023-44267**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	9.8	Online Art Gallery v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'gender' parameter of the header.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-44268**	N/A	A-PRO-ONLI-241123/1399
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Oct-2023	9.8	Online Art Gallery v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'add1' parameter of the header.php resource does not validate the characters received and they are sent unfiltered to the database.	N/A	A-PRO-ONLI-241123/1400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-44375		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Oct-2023	9.8	Online Art Gallery v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'add2' parameter of the header.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-44376**	N/A	A-PRO-ONLI-241123/1401
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Oct-2023	9.8	Online Art Gallery v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'add3' parameter of the header.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-44377**	N/A	A-PRO-ONLI-241123/1402
Vendor: Proxmox					
Product: proxmox					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 4.0.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Oct-2023	6.1	Proxmox proxmox-widget-toolkit before 4.0.9, as used in multiple Proxmox products, allows XSS via the edit notes feature. **CVE ID : CVE-2023-46854**	https://pve.proxmox.com/wiki/Package_Repositories#sysadmin_test_repo	A-PRO-PROX-241123/1403
Vendor: pwncyn					
Product: fancms					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	6.1	Cross Site Scripting vulnerability in FanCMS v.1.0.0 allows an attacker to execute arbitrary code via the content1 parameter in the demo.php file. **CVE ID : CVE-2023-46505**	N/A	A-PWN-FANC-241123/1404
Product: yxbookcms					
Affected Version(s): 1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	6.1	Cross Site Scripting (XSS) vulnerability in PwnCYN YXBOOKCMS v.1.0.2 allows a remote attacker to execute arbitrary code via the reader management and book input modules. **CVE ID : CVE-2023-46503**	https://github.com/PwnCYN/YXBOOKCMS/issues/2	A-PWN-YXBO-241123/1405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	5.4	Cross Site Scripting (XSS) vulnerability in PwnCYN YXBOOKCMS v.1.0.2 allows a physically proximate attacker to execute arbitrary code via the library name function in the general settings component. **CVE ID : CVE-2023-46504**	https://github.com/PwnCYN/YXBOOKCMS/issues/1	A-PWN-YXBO-241123/1406
Vendor: pypa					
Product: pip					
Affected Version(s): * Up to (excluding) 23.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	3.3	When installing a package from a Mercurial VCS URL (ie "pip install hg+...") with pip prior to v23.3, the specified Mercurial revision could be used to inject arbitrary configuration options to the "hg clone" call (ie "--config"). Controlling the Mercurial configuration can modify how and which repository is installed. This vulnerability does not	https://mail.python.org/archives/list/security-announce@python.org/thread/F4PL35U6X4VVHZ5ILJU3PWUWN7H7LZXL/, https://github.com/pypa/pip/pull/12306	A-PYP-PIP-241123/1407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affect users who aren't installing from Mercurial. **CVE ID : CVE-2023-5752**		
Vendor: Python					
Product: urllib3					
Affected Version(s): * Up to (excluding) 1.26.18					
Exposure of Sensitive Information to an Unauthorized Actor	17-Oct-2023	4.2	urllib3 is a user-friendly HTTP client library for Python. urllib3 previously wouldn't remove the HTTP request body when an HTTP redirect response using status 301, 302, or 303 after the request had its method changed from one that could accept a request body (like `POST`) to `GET` as is required by HTTP RFCs. Although this behavior is not specified in the section for redirects, it can be inferred by piecing together information from different sections and we have observed the behavior in other major HTTP client implementations	https://github.com/urllib3/urllib3/commit/4e98d57809dacab1cbe625fddeec1a290c478ea9	A-PYT-URLL-241123/1408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			like curl and web browsers. Because the vulnerability requires a previously trusted service to become compromised in order to have an impact on confidentiality we believe the exploitability of this vulnerability is low. Additionally, many users aren't putting sensitive data in HTTP request bodies, if this is the case then this vulnerability isn't exploitable. Both of the following conditions must be true to be affected by this vulnerability: 1. Using urllib3 and submitting sensitive information in the HTTP request body (such as form data or JSON) and 2. The origin service is compromised and starts redirecting using 301, 302, or 303 to a malicious peer or the redirected-to service becomes compromised. This issue has been		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addressed in versions 1.26.18 and 2.0.7 and users are advised to update to resolve this issue. Users unable to update should disable redirects for services that aren't expecting to respond with redirects with `redirects=False` and disable automatic redirects with `redirects=False` and handle 301, 302, and 303 redirects manually by stripping the HTTP request body. **CVE ID : CVE-2023-45803**		
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.0.7					
Exposure of Sensitive Information to an Unauthorized Actor	17-Oct-2023	4.2	urllib3 is a user-friendly HTTP client library for Python. urllib3 previously wouldn't remove the HTTP request body when an HTTP redirect response using status 301, 302, or 303 after the request had its method changed from one that could	https://github.com/urllib3/urllib3/commit/4e98d57809dacab1cbe625fddeec1a290c478ea9	A-PYT-URLL-241123/1409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accept a request body (like `POST`) to `GET` as is required by HTTP RFCs. Although this behavior is not specified in the section for redirects, it can be inferred by piecing together information from different sections and we have observed the behavior in other major HTTP client implementations like curl and web browsers. Because the vulnerability requires a previously trusted service to become compromised in order to have an impact on confidentiality we believe the exploitability of this vulnerability is low. Additionally, many users aren't putting sensitive data in HTTP request bodies, if this is the case then this vulnerability isn't exploitable. Both of the following conditions must be true to be affected by this		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability: 1. Using urllib3 and submitting sensitive information in the HTTP request body (such as form data or JSON) and 2. The origin service is compromised and starts redirecting using 301, 302, or 303 to a malicious peer or the redirected-to service becomes compromised. This issue has been addressed in versions 1.26.18 and 2.0.7 and users are advised to update to resolve this issue. Users unable to update should disable redirects for services that aren't expecting to respond with redirects with `redirects=False` and disable automatic redirects with `redirects=False` and handle 301, 302, and 303 redirects manually by stripping the HTTP request body.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45803		
Vendor: qad					
Product: search_server					
Affected Version(s): * Up to (excluding) 1.0.0.315					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	The QAD Search Server is vulnerable to Stored Cross-Site Scripting (XSS) in versions up to, and including, 1.0.0.315 due to insufficient checks on indexes. This makes it possible for unauthenticated attackers to create a new index and inject a malicious web script into its name, that will execute whenever a user accesses the search page. **CVE ID : CVE-2023-45471**	N/A	A-QAD-SEAR-241123/1410
Vendor: Qnap					
Product: qusbcam2					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.0.3					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Oct-2023	8.8	An OS command injection vulnerability has been reported to affect QUSBCam2. If exploited, the vulnerability could allow users to execute commands via a network.	https://www.qnap.com/en/security-advisory/qsa-23-43	A-QNA-QUSB-241123/1411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			We have already fixed the vulnerability in the following version: QUSBCam2 2.0.3 (2023/06/15) and later **CVE ID : CVE-2023-23373**		
Vendor: qrokes					
Product: qr_twitter_widget					
Affected Version(s): * Up to (including) 0.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in QROkes QR Twitter Widget plugin <= 0.2.3 versions. **CVE ID : CVE-2023-45628**	N/A	A-QRO-QR_T-241123/1412
Vendor: quantumcloud					
Product: ai_chatbot					
Affected Version(s): * Up to (excluding) 4.9.1					
N/A	19-Oct-2023	8.1	The AI ChatBot plugin for WordPress is vulnerable to Arbitrary File Deletion in versions up to, and including, 4.8.9 as well as version 4.9.2. This makes it possible for authenticated attackers with subscriber privileges to delete	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2977505%40chatbot%2Ftrunk&old=2967435%40chatbot%2Ftrunk&sfp_email=&sfph_mail=	A-QUA-AI_C-241123/1413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary files on the server, which makes it possible to take over affected sites as well as others sharing the same hosting account. Version 4.9.1 originally addressed the issue, but it was reintroduced in 4.9.2 and fixed again in 4.9.3. **CVE ID : CVE-2023-5212**		
N/A	19-Oct-2023	8.1	The AI ChatBot for WordPress is vulnerable to Directory Traversal in versions up to, and including, 4.8.9 as well as 4.9.2 via the qcld_openai_upload_pagetraining_file function. This allows subscriber-level attackers to append "<?php" to any existing file on the server resulting in potential DoS when appended to critical files such as wp-config.php. **CVE ID : CVE-2023-5241**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2977505%40chatbot%2Ftrunk&old=2967435%40chatbot%2Ftrunk&sfp_email=&sfph_mail=	A-QUA-AI_C-241123/1414
N/A	19-Oct-2023	7.5	The ChatBot plugin for WordPress is vulnerable to SQL Injection via the	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfp	A-QUA-AI_C-241123/1415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			$strid parameter in versions up to, and including, 4.8.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-5204**	h_mail=&repon ame=&new=29 77505%40chat bot%2Ftrunk&o ld=2967435%4 0chatbot%2Ftr unk&sfp_email= &sfph_mail=	
N/A	19-Oct-2023	5.3	The ChatBot plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 4.8.9 via the qcld_wb_chatbot_c heck_user function. This can allow unauthenticated attackers to extract sensitive data including confirmation as to whether a user name exists on the	https://plugins. trac.wordpress. org/changeset? sfp_email=&sfp h_mail=&repon ame=&new=29 77505%40chat bot%2Ftrunk&o ld=2967435%4 0chatbot%2Ftr unk&sfp_email= &sfph_mail=	A-QUA-AI_C-241123/1416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			site as well as order information for existing users. **CVE ID : CVE-2023-5254**		
Affected Version(s): * Up to (including) 4.8.9					
Missing Authorization	20-Oct-2023	9.8	The AI ChatBot plugin for WordPress is vulnerable to unauthorized use of AJAX actions due to missing capability checks on the corresponding functions in versions up to, and including, 4.8.9 as well as 4.9.2. This makes it possible for unauthenticated attackers to perform some of those actions that were intended for higher privileged users. **CVE ID : CVE-2023-5533**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2977505%40chatbot%2Ftrunk&old=2967435%40chatbot%2Ftrunk&sfp_email=&sfph_mail=	A-QUA-AI_C-241123/1417
Cross-Site Request Forgery (CSRF)	20-Oct-2023	5.4	The AI ChatBot plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.8.9 and 4.9.2. This is due to missing or incorrect nonce	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2977505%40chatbot%2Ftrunk&old=2967435%40chatbot%2Ftr	A-QUA-AI_C-241123/1418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation on the corresponding functions. This makes it possible for unauthenticated attackers to invoke those functions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-5534**	unk&sfp_email=&sfph_mail=	
Affected Version(s): 4.9.2					
Missing Authorization	20-Oct-2023	9.8	The AI ChatBot plugin for WordPress is vulnerable to unauthorized use of AJAX actions due to missing capability checks on the corresponding functions in versions up to, and including, 4.8.9 as well as 4.9.2. This makes it possible for unauthenticated attackers to perform some of those actions that were intended for higher privileged users.	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2977505%40chatbot%2Ftrunk&old=2967435%40chatbot%2Ftrunk&sfp_email=&sfph_mail=	A-QUA-AI_C-241123/1419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5533		
N/A	19-Oct-2023	8.1	The AI ChatBot plugin for WordPress is vulnerable to Arbitrary File Deletion in versions up to, and including, 4.8.9 as well as version 4.9.2. This makes it possible for authenticated attackers with subscriber privileges to delete arbitrary files on the server, which makes it possible to take over affected sites as well as others sharing the same hosting account. Version 4.9.1 originally addressed the issue, but it was reintroduced in 4.9.2 and fixed again in 4.9.3. **CVE ID : CVE-2023-5212**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2977505%40chatbot%2Ftrunk&old=2967435%40chatbot%2Ftrunk&sfp_email=&sfph_mail=	A-QUA-AI_C-241123/1420
N/A	19-Oct-2023	8.1	The AI ChatBot for WordPress is vulnerable to Directory Traversal in versions up to, and including, 4.8.9 as well as 4.9.2 via the qcld_openai_uploa	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2977505%40chatbot%2Ftrunk&old=2967435%4	A-QUA-AI_C-241123/1421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			d_pagetraining_file function. This allows subscriber-level attackers to append "<?php" to any existing file on the server resulting in potential DoS when appended to critical files such as wp-config.php. **CVE ID : CVE-2023-5241**	0chatbot%2Ftrunk&sfp_email=&sfph_mail=	
Cross-Site Request Forgery (CSRF)	20-Oct-2023	5.4	The AI ChatBot plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.8.9 and 4.9.2. This is due to missing or incorrect nonce validation on the corresponding functions. This makes it possible for unauthenticated attackers to invoke those functions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-5534**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2977505%40chatbot%2Ftrunk&old=2967435%40chatbot%2Ftrunk&sfp_email=&sfph_mail=	A-QUA-AI_C-241123/1422
Vendor: qwerty23					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: rocket_font					
Affected Version(s): * Up to (including) 1.2.3					
Cross-Site Request Forgery (CSRF)	21-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Qwerty23 Rocket Font plugin <= 1.2.3 versions. **CVE ID : CVE-2023-46067**	N/A	A-QWE-ROCK-241123/1423
Vendor: Radare					
Product: radare2					
Affected Version(s): * Up to (excluding) 5.9.0					
Out-of-bounds Read	28-Oct-2023	9.8	An out-of-bounds read in radare2 v.5.8.9 and before exists in the print_insn32_fpu function of libr/arch/p/nds32/nds32-dis.h. **CVE ID : CVE-2023-46569**	N/A	A-RAD-RADA-241123/1424
Out-of-bounds Read	28-Oct-2023	9.8	An out-of-bounds read in radare2 v.5.8.9 and before exists in the print_insn32 function of libr/arch/p/nds32/nds32-dis.h. **CVE ID : CVE-2023-46570**	N/A	A-RAD-RADA-241123/1425
Out-of-bounds Write	20-Oct-2023	8.8	Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.9.0. **CVE ID : CVE-2023-5686**	https://huntr.com/bounties/bbfe1f76-8fa1-4a8c-909d-65b16e970be0, https://github.com/radareorg/	A-RAD-RADA-241123/1426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				radare2/commit/1bdda93e348c160c84e30da3637acef26d0348de	
Vendor: ravanh					
Product: skype_legacy_buttons					
Affected Version(s): * Up to (including) 3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	The Skype Legacy Buttons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'skype-status' shortcode in all versions up to, and including, 3.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5615**	N/A	A-RAV-SKYP-241123/1427
Vendor: redis					
Product: redis					
Affected Version(s): 2.6.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	18-Oct-2023	3.6	Redis is an in-memory database that persists on disk. On startup, Redis begins listening on a Unix socket before adjusting its permissions to the user-provided configuration. If a permissive umask(2) is used, this creates a race condition that enables, during a short period of time, another process to establish an otherwise unauthorized connection. This problem has existed since Redis 2.6.0-RC1. This issue has been addressed in Redis versions 7.2.2, 7.0.14 and 6.2.14. Users are advised to upgrade. For users unable to upgrade, it is possible to work around the problem by disabling Unix sockets, starting Redis with a restrictive umask, or storing the Unix socket file in a	https://github.com/redis/redis/commit/03345ddc7faf7af079485f2cbe5d17a1611cbce1, https://github.com/redis/redis/security/advisories/GHSA-ghmp-889m-7cvx	A-RED-REDI-241123/1428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected directory. **CVE ID : CVE-2023-45145**		
Affected Version(s): From (including) 2.6.0 Up to (excluding) 6.2.14					
Exposure of Resource to Wrong Sphere	18-Oct-2023	3.6	Redis is an in-memory database that persists on disk. On startup, Redis begins listening on a Unix socket before adjusting its permissions to the user-provided configuration. If a permissive umask(2) is used, this creates a race condition that enables, during a short period of time, another process to establish an otherwise unauthorized connection. This problem has existed since Redis 2.6.0-RC1. This issue has been addressed in Redis versions 7.2.2, 7.0.14 and 6.2.14. Users are advised to upgrade. For users unable to upgrade, it is possible to work around the problem by disabling Unix	https://github.com/redis/redis/commit/03345ddc7faf7af079485f2cbe5d17a1611cbce1, https://github.com/redis/redis/security/advisories/GHSA-ghmp-889m-7cvx	A-RED-REDI-241123/1429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sockets, starting Redis with a restrictive umask, or storing the Unix socket file in a protected directory. **CVE ID : CVE-2023-45145**		
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.14					
Exposure of Resource to Wrong Sphere	18-Oct-2023	3.6	Redis is an in-memory database that persists on disk. On startup, Redis begins listening on a Unix socket before adjusting its permissions to the user-provided configuration. If a permissive umask(2) is used, this creates a race condition that enables, during a short period of time, another process to establish an otherwise unauthorized connection. This problem has existed since Redis 2.6.0-RC1. This issue has been addressed in Redis versions 7.2.2, 7.0.14 and 6.2.14. Users are advised to upgrade. For users unable to	https://github.com/redis/redis/commit/03345ddc7faf7af079485f2cbe5d17a1611cbce1, https://github.com/redis/redis/security/advisories/GHSA-ghmp-889m-7cvx	A-RED-REDI-241123/1430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade, it is possible to work around the problem by disabling Unix sockets, starting Redis with a restrictive umask, or storing the Unix socket file in a protected directory. **CVE ID : CVE-2023-45145**		
Affected Version(s): From (including) 7.2.0 Up to (excluding) 7.2.2					
Exposure of Resource to Wrong Sphere	18-Oct-2023	3.6	Redis is an in-memory database that persists on disk. On startup, Redis begins listening on a Unix socket before adjusting its permissions to the user-provided configuration. If a permissive umask(2) is used, this creates a race condition that enables, during a short period of time, another process to establish an otherwise unauthorized connection. This problem has existed since Redis 2.6.0-RC1. This issue has been addressed in Redis	https://github.com/redis/redis/commit/03345ddc7faf7af079485f2cbe5d17a1611cbce1, https://github.com/redis/redis/security/advisories/GHSA-ghmp-889m-7cvx	A-RED-REDI-241123/1431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 7.2.2, 7.0.14 and 6.2.14. Users are advised to upgrade. For users unable to upgrade, it is possible to work around the problem by disabling Unix sockets, starting Redis with a restrictive umask, or storing the Unix socket file in a protected directory. **CVE ID : CVE-2023-45145**		
Vendor: rednao					
Product: woocommerce_pdf_invoice_builder					
Affected Version(s): * Up to (including) 1.2.102					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in RedNao WooCommerce PDF Invoice Builder, Create invoices, packing slips and more plugin <= 1.2.102 versions. **CVE ID : CVE-2023-46076**	N/A	A-RED-WOOC-241123/1432
Vendor: Relative					
Product: synchrony					
Affected Version(s): From (including) 2.0.1 Up to (excluding) 2.4.4					
Improperly Controlled Modificatio	17-Oct-2023	7.8	Synchrony deobfuscator is a javascript cleaner	https://github.com/relative/synchrony/commi	A-REL-SYNC-241123/1433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n of Object Prototype Attributes ('Prototype Pollution')			& deobfuscator. A `__proto__` pollution vulnerability exists in versions before v2.4.4. Successful exploitation could lead to arbitrary code execution. A `__proto__` pollution vulnerability exists in the `LiteralMap` transformer allowing crafted input to modify properties in the Object prototype. A fix has been released in `deobfuscator@2.4.4`. Users are advised to upgrade. Users unable to upgrade should launch node with the [--disable-proto=delete][disable-proto] or [--disable-proto=throw][disable-proto] flags **CVE ID : CVE-2023-45811**	t/b583126be94c4db7c5a478f1c5204bfb4162cf40, https://github.com/relative/synchrony/security/advisories/GHSA-jg82-xh3w-rhxx	
Vendor: remark42					
Product: remark42					
Affected Version(s): * Up to (including) 1.12.1					
Server-Side Request	23-Oct-2023	7.5	umputun remark42 version 1.12.1 and before has a Blind Server-	N/A	A-REM-REMA-241123/1434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			Side Request Forgery (SSRF) vulnerability. **CVE ID : CVE-2023-45966**		
Vendor: remyandrade					
Product: file_manager_app					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	26-Oct-2023	9.8	A vulnerability classified as critical was found in SourceCodester File Manager App 1.0. Affected by this vulnerability is an unknown functionality of the file endpoint/add-file.php. The manipulation of the argument uploadedFileName leads to unrestricted upload. 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-243595. **CVE ID : CVE-2023-5790**	N/A	A-REM-FILE-241123/1435
Product: sticky_notes_app					
Affected Version(s): 1.0					
Improper Neutralizat	26-Oct-2023	9.8	A vulnerability has been found in	N/A	A-REM-STIC-241123/1436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			SourceCodester Sticky Notes App 1.0 and classified as critical. This vulnerability affects unknown code of the file endpoint/delete-note.php. The manipulation of the argument note leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-243598 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-5792**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2023	6.1	A vulnerability, which was classified as problematic, was found in SourceCodester Sticky Notes App 1.0. This affects an unknown part of the file endpoint/add-note.php. The manipulation of the argument noteTitle/noteContent leads to cross site scripting. It is possible to initiate	N/A	A-REM-STIC-241123/1437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-243597 was assigned to this vulnerability. **CVE ID : CVE-2023-5791**		
Vendor: rewweb					
Product: bbp_style_pack					
Affected Version(s): * Up to (excluding) 5.6.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Robin Wilson bbp style pack plugin <= 5.6.7 versions. **CVE ID : CVE-2023-44984**	N/A	A-REW-BBP_-241123/1438
Vendor: Ritecms					
Product: ritecms					
Affected Version(s): 3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	4.8	A File upload vulnerability in RiteCMS 3.0 allows a local attacker to upload a SVG file with XSS content. **CVE ID : CVE-2023-44767**	N/A	A-RIT-RITE-241123/1439
Vendor: rmagick					
Product: rmagick					
Affected Version(s): * Up to (excluding) 5.3.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	30-Oct-2023	3.3	A memory leak flaw was found in ruby-magick, an interface between Ruby and ImageMagick. This issue can lead to a denial of service (DOS) by memory exhaustion. **CVE ID : CVE-2023-5349**	https://github.com/rmagick/rmagick/pull/1406	A-RMA-RMAG-241123/1440
Vendor: Rockwellautomation					
Product: arena_simulation					
Affected Version(s): * Up to (excluding) 16.20.02					
Out-of-bounds Read	27-Oct-2023	7.8	An arbitrary code execution vulnerability was reported to Rockwell Automation in Arena Simulation that could potentially allow a malicious user to commit unauthorized arbitrary code to the software by using a memory buffer overflow. The threat-actor could then execute malicious code on the system affecting the confidentiality, integrity, and availability of the product. The user	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1141145	A-ROC-AREN-241123/1441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would need to open a malicious file provided to them by the attacker for the code to execute. **CVE ID : CVE-2023-27854**		
Access of Uninitialized Pointer	27-Oct-2023	7.8	Rockwell Automation Arena Simulation contains an arbitrary code execution vulnerability that could potentially allow a malicious user to commit unauthorized code to the software by using an uninitialized pointer in the application. The threat-actor could then execute malicious code on the system affecting the confidentiality, integrity, and availability of the product. The user would need to open a malicious file provided to them by the	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1141145	A-ROC-AREN-241123/1442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker for the code to execute. **CVE ID : CVE-2023-27858**		
Product: factorytalk_services_platform					
Affected Version(s): * Up to (excluding) 2.80					
Improper Authentication	27-Oct-2023	8.1	Due to inadequate code logic, a previously unauthenticated threat actor could potentially obtain a local Windows OS user token through the FactoryTalk® Services Platform web service and then use the token to log in into FactoryTalk® Services Platform . This vulnerability can only be exploited if the authorized user did not previously log in into the FactoryTalk® Services Platform web service. **CVE ID : CVE-2023-46290**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1141165	A-ROC-FACT-241123/1443
Product: factorytalk_view					
Affected Version(s): From (including) 11.0 Up to (including) 13.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	27-Oct-2023	7.5	Rockwell Automation FactoryTalk View Site Edition insufficiently validates user input, which could potentially allow threat actors to send malicious data bringing the product offline. If exploited, the product would become unavailable and require a restart to recover resulting in a denial-of-service condition. **CVE ID : CVE-2023-46289**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1141167	A-ROC-FACT-241123/1444
Vendor: Roundcube					
Product: webmail					
Affected Version(s): * Up to (excluding) 1.4.15					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	5.4	Roundcube before 1.4.15, 1.5.x before 1.5.5, and 1.6.x before 1.6.4 allows stored XSS via an HTML e-mail message with a crafted SVG document because of program/lib/Roundcube/rcube_wash	https://github.com/roundcube/roundcubemail/commit/6ee6e7ae301e165e2b2cb703edf75552e5376613, https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1054079, https://github.c	A-ROU-WEBM-241123/1445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tml.php behavior. This could allow a remote attacker to load arbitrary JavaScript code. **CVE ID : CVE-2023-5631**	om/roundcube/roundcubemail/commit/41756cc3331b495cc0b71886984474dc529dd31d	
Affected Version(s): From (including) 1.5.0 Up to (excluding) 1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	5.4	Roundcube before 1.4.15, 1.5.x before 1.5.5, and 1.6.x before 1.6.4 allows stored XSS via an HTML e-mail message with a crafted SVG document because of program/lib/Roundcube/rcube_washtml.php behavior. This could allow a remote attacker to load arbitrary JavaScript code.	https://github.com/roundcube/roundcubemail/commit/6ee6e7ae301e165e2b2cb703edf75552e5376613, https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1054079, https://github.com/roundcube/roundcubemail/commit/41756cc3331b495cc0b71886984474dc529dd31d	A-ROU-WEBM-241123/1446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5631		
Affected Version(s): From (including) 1.6.0 Up to (excluding) 1.6.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	5.4	Roundcube before 1.4.15, 1.5.x before 1.5.5, and 1.6.x before 1.6.4 allows stored XSS via an HTML e-mail message with a crafted SVG document because of program/lib/Roundcube/rcube_washtml.php behavior. This could allow a remote attacker to load arbitrary JavaScript code.	https://github.com/roundcube/roundcubemail/commit/6ee6e7ae301e165e2b2cb703edf75552e5376613, https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1054079, https://github.com/roundcube/roundcubemail/commit/41756cc3331b495cc0b71886984474dc529dd31d	A-ROU-WEBM-241123/1447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5631		
Vendor: salesmanago					
Product: salesmanago					
Affected Version(s): * Up to (including) 3.2.4					
Improper Authentication	21-Oct-2023	5.3	The SALESmanago plugin for WordPress is vulnerable to Log Injection in versions up to, and including, 3.2.4. This is due to the use of a weak authentication token for the /wp-json/salesmanago/v1/callbackApiV3 API endpoint which is simply a SHA1 hash of the site URL and client ID found in the page source of the website. This makes it possible for unauthenticated attackers to inject arbitrary content into the log files, and when combined with another vulnerability this could have significant consequences. **CVE ID : CVE-2023-4939**	https://plugins.trac.wordpress.org/browser/salesmanago/trunk/src/Includes/Helper.php#L376	A-SAL-SALE-241123/1448
Vendor: saleswizard					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nsc					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	6.1	The nsc theme for WordPress is vulnerable to Reflected Cross-Site Scripting via prototype pollution in versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2023-3965**	N/A	A-SAL-NSC-241123/1449
Vendor: Samba					
Product: samba					
Affected Version(s): * Up to (excluding) 4.19.2					
Out-of-bounds Write	25-Oct-2023	6.5	A heap-based Buffer Overflow flaw was discovered in Samba. It could allow a remote, authenticated attacker to exploit this vulnerability	https://bugzilla.samba.org/show_bug.cgi?id=15491	A-SAM-SAMB-241123/1450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to cause a denial of service. **CVE ID : CVE-2023-5568**		
Vendor: saml_project					
Product: saml					
Affected Version(s): * Up to (excluding) 0.4.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-2023	6.1	github.com/crewjam/saml is a saml library for the go language. In affected versions the package does not validate the ACS Location URI according to the SAML binding being parsed. If abused, this flaw allows attackers to register malicious Service Providers at the IdP and inject Javascript in the ACS endpoint definition, achieving Cross-Site-Scripting (XSS) in the IdP context during the redirection at the end of a SAML SSO Flow. Consequently, an attacker may perform any authenticated action as the victim once the victim's browser loaded the SAML IdP initiated SSO link for the	https://github.com/crewjam/saml/commit/b07b16cf83c4171d16da4d85608cb827f183cd79, https://github.com/crewjam/saml/security/advisories/GHSA-267v-3v32-g6q5	A-SAM-SAML-241123/1451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious service provider. Note: SP registration is commonly an unrestricted operation in IdPs, hence not requiring particular permissions or publicly accessible to ease the IdP interoperability. This issue is fixed in version 0.4.14. Users unable to upgrade may perform external validation of URLs provided in SAML metadata, or restrict the ability for end-users to upload arbitrary metadata. **CVE ID : CVE-2023-45683**		
Vendor: santesoft					
Product: dicom_viewer_pro					
Affected Version(s): * Up to (excluding) 12.2.6					
Out-of-bounds Write	19-Oct-2023	7.8	Sante DICOM Viewer Pro lacks proper validation of user-supplied data when parsing DICOM files. This could lead to a stack-based buffer overflow. An attacker could leverage this	N/A	A-SAN-DICO-241123/1452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-35986**		
Out-of-bounds Write	19-Oct-2023	7.8	Sante DICOM Viewer Pro lacks proper validation of user-supplied data when parsing DICOM files. This could lead to an out-of-bounds write. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-39431**	N/A	A-SAN-DICO-241123/1453
Product: fft_imaging					
Affected Version(s): * Up to (excluding) 1.4.1					
Out-of-bounds Read	19-Oct-2023	7.8		N/A	A-SAN-FFT_-241123/1454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Santesoft Sante FFT Imaging lacks proper validation of user-supplied data when parsing DICOM files. This could lead to an out-of-bounds read. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-5059**		
Vendor: SAP					
Product: enable_now_enable_now_consump_del					
Affected Version(s): 1704					
Improper Restriction of Rendered UI Layers or Frames	30-Oct-2023	6.1	In SAP Enable Now - versions WPB_MANAGER 1.0, WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704, the X-FRAME-OPTIONS response header is not implemented, allowing an unauthenticated attacker to attempt clickjacking, which could result in disclosure or	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-ENAB-241123/1455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modification of information. **CVE ID : CVE-2023-36920**		
Product: enable_now_wpb_manager					
Affected Version(s): 1.0					
Improper Restriction of Rendered UI Layers or Frames	30-Oct-2023	6.1	In SAP Enable Now - versions WPB_MANAGER 1.0, WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704, the X-FRAME-OPTIONS response header is not implemented, allowing an unauthenticated attacker to attempt clickjacking, which could result in disclosure or modification of information. **CVE ID : CVE-2023-36920**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-ENAB-241123/1456
Product: enable_now_wpb_manager_ce					
Affected Version(s): 10					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Rendered UI Layers or Frames	30-Oct-2023	6.1	In SAP Enable Now - versions WPB_MANAGER 1.0, WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704, the X-FRAME-OPTIONS response header is not implemented, allowing an unauthenticated attacker to attempt clickjacking, which could result in disclosure or modification of information. **CVE ID : CVE-2023-36920**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-ENAB-241123/1457
Product: enable_now_wpb_manager_hana					
Affected Version(s): 10					
Improper Restriction of Rendered UI Layers or Frames	30-Oct-2023	6.1	In SAP Enable Now - versions WPB_MANAGER 1.0, WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704, the X-FRAME-OPTIONS response header is not	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-ENAB-241123/1458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implemented, allowing an unauthenticated attacker to attempt clickjacking, which could result in disclosure or modification of information. **CVE ID : CVE-2023-36920**		
Vendor: sayandatta					
Product: simple_posts_ticker					
Affected Version(s): * Up to (excluding) 1.1.6					
N/A	16-Oct-2023	5.4	The Simple Posts Ticker WordPress plugin before 1.1.6 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-4646**	N/A	A-SAY-SIMP-241123/1459
N/A	16-Oct-2023	4.8	The Simple Posts Ticker WordPress plugin before 1.1.6	N/A	A-SAY-SIMP-241123/1460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-4725**		
Vendor: sazzadh					
Product: testimonial_slider_shortcode					
Affected Version(s): * Up to (excluding) 1.1.9					
N/A	16-Oct-2023	5.4	The Testimonial Slider Shortcode WordPress plugin before 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admin **CVE ID : CVE-2023-4795**	N/A	A-SAZ-TEST-241123/1461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: scala-sbt					
Product: io					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.9.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Oct-2023	7.1	sbt is a build tool for Scala, Java, and others. Given a specially crafted zip or JAR file, `IO.unzip` allows writing of arbitrary file. This would have potential to overwrite `/root/.ssh/authorized_keys`. Within sbt's main code, `IO.unzip` is used in `pullRemoteCache` task and `Resolvers.remote`; however many projects use `IO.unzip(...)` directly to implement custom tasks. This vulnerability has been patched in version 1.9.7. **CVE ID : CVE-2023-46122**	https://github.com/sbt/io/issues/358, https://github.com/sbt/sbt/security/advisories/GHSA-h9mw-grgx-2fhf, https://github.com/sbt/io/commit/124538348db0713c80793cb57b915f97ec13188a, https://github.com/sbt/io/pull/360	A-SCA-IO-241123/1462
Product: sbt					
Affected Version(s): From (including) 0.3.4 Up to (excluding) 1.9.7					
Improper Limitation of a Pathname to a Restricted Directory	23-Oct-2023	7.1	sbt is a build tool for Scala, Java, and others. Given a specially crafted zip or JAR file, `IO.unzip` allows writing of arbitrary file. This would have potential to	https://github.com/sbt/io/issues/358, https://github.com/sbt/sbt/security/advisories/GHSA-h9mw-grgx-2fhf, https://github.c	A-SCA-SBT-241123/1463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			overwrite `/root/.ssh/authorized_keys`. Within sbt's main code, `IO.unzip` is used in `pullRemoteCache` task and `Resolvers.remote`; however many projects use `IO.unzip(...)` directly to implement custom tasks. This vulnerability has been patched in version 1.9.7. **CVE ID : CVE-2023-46122**	om/sbt/io/commit/124538348db0713c80793cb57b915f97ec13188a, https://github.com/sbt/io/pull/360	
Vendor: scribit					
Product: proofreading					
Affected Version(s): * Up to (including) 1.0.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Scribit Proofreading plugin <= 1.0.11 versions. **CVE ID : CVE-2023-45772**	N/A	A-SCR-PROO-241123/1464
Vendor: seacms					
Product: seacms					
Affected Version(s): * Up to (including) 12.9					
N/A	25-Oct-2023	9.8	An issue in SeaCMS v.12.9 allows an attacker to execute arbitrary commands via the	N/A	A-SEA-SEAC-241123/1465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin_safe.php component. **CVE ID : CVE-2023-46010**		
Vendor: secondlinethemes					
Product: podcast_subscribe_buttons					
Affected Version(s): * Up to (including) 1.4.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	The Podcast Subscribe Buttons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'podcast_subscribe' shortcode in versions up to, and including, 1.4.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5308**	https://plugins.trac.wordpress.org/browser/podcast-subscribe-buttons/tags/1.4.8/template-parts/inline-button.php#L30 , https://plugins.trac.wordpress.org/changeset/2973904/podcast-subscribe-buttons#file529	A-SEC-PODC-241123/1466
Vendor: secudos					
Product: qiata					
Affected Version(s): 4.13					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	20-Oct-2023	7.8	SECUDOS Qiata (DOMOS OS) 4.13 has Insecure Permissions for the previewRm.sh daily cronjob. To exploit this, an attacker needs access as a low-privileged user to the underlying DOMOS system. Every user on the system has write permission for previewRm.sh, which is executed by the root user. **CVE ID : CVE-2023-40361**	N/A	A-SEC-QIAT-241123/1467
Vendor: securepoint					
Product: openvpn-client					
Affected Version(s): * Up to (excluding) 2.0.40					
N/A	30-Oct-2023	7.8	The installer (aka openvpn-client-installer) in Securepoint SSL VPN Client before 2.0.40 allows local privilege escalation during installation or repair. **CVE ID : CVE-2023-47101**	N/A	A-SEC-OPEN-241123/1468
Vendor: seedprod					
Product: rafflepress					
Affected Version(s): * Up to (including) 1.12.0					
Improper Neutralization of Input	30-Oct-2023	5.4	The Giveaways and Contests by RafflePress plugin for WordPress is	https://plugins.trac.wordpress.org/browser/rafflepress/tags/1	A-SEE-RAFF-241123/1469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			vulnerable to Stored Cross-Site Scripting via the 'rafflepress' and 'rafflepress_gutenberg' shortcode in versions up to, and including, 1.12.0 due to insufficient input sanitization and output escaping on 'giframe' user supplied attribute. This makes it possible for authenticated attackers with contributor level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5049**	.11.4/app/rafflepress.php#L955, https://plugins.trac.wordpress.org/changeset/2976620/rafflepress#file0	
Product: website_builder_by_seedprod					
Affected Version(s): * Up to (including) 6.15.13.1					
Cross-Site Request Forgery (CSRF)	20-Oct-2023	4.3	The Website Builder by SeedProd plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 6.15.13.1. This is due to missing or incorrect nonce	https://plugins.trac.wordpress.org/browser/coming-soon/trunk/resources/views/builder.php#L164, https://plugins.trac.wordpress.org/changeset/2968455/comin	A-SEE-WEBS-241123/1470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation on functionality in the builder.php file. This makes it possible for unauthenticated attackers to change the stripe connect token via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-4975**	g-soon/trunk/resources/views/builder.php	
Vendor: sendpulse					
Product: free_web_push					
Affected Version(s): * Up to (including) 1.3.1					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in SendPulse SendPulse Free Web Push plugin <= 1.3.1 versions. **CVE ID : CVE-2023-45274**	N/A	A-SEN-FREE-241123/1471
Vendor: sevenspark					
Product: bellows_accordion_menu					
Affected Version(s): * Up to (including) 1.4.2					
Improper Neutralization of Input During Web Page Generation	30-Oct-2023	5.4	The Bellows Accordion Menu plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and	https://plugins.trac.wordpress.org/browser/bellows-accordion-menu/tags/1.4.2/includes/bellows.api.php#L5,	A-SEV-BELL-241123/1472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			including, 1.4.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5164**	https://plugins.trac.wordpress.org/browser/bellows-accordion-menu/tags/1.4.2/includes/functions.php#L12	
Vendor: sfu					
Product: open_journal_system					
Affected Version(s): * Up to (excluding) 3.3.0-16					
Cross-Site Request Forgery (CSRF)	18-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) in GitHub repository pkp/ojs prior to 3.3.0-16. **CVE ID : CVE-2023-5626**	https://github.com/pkp/ojs/commit/99a9f393190383454aa5ddffedffc89596f6c682, https://huntr.dev/bounties/c99279c1-709a-4e7b-a042-010c2bb44d6b	A-SFU-OPEN-241123/1473
Vendor: shopfiles					
Product: ebook_store					
Affected Version(s): * Up to (including) 5.785					
Improper Neutralization of	18-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability	N/A	A-SHO-EBOO-241123/1474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			in Shopfiles Ltd Ebook Store plugin <= 5.785 versions. **CVE ID : CVE-2023-45602**		
Vendor: shortcode_menu_project					
Product: shortcod_menu					
Affected Version(s): * Up to (including) 3.2					
N/A	30-Oct-2023	5.4	The Shortcode Menu plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'shortmenu' shortcode in versions up to, and including, 3.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5565**	N/A	A-SHO-SHOR-241123/1475
Vendor: shortpixel					
Product: enable_media_replace					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 4.1.3					
N/A	16-Oct-2023	8.8	The Enable Media Replace WordPress plugin before 4.1.3 unserializes user input via the Remove Background feature, which could allow Author+ users to perform PHP Object Injection when a suitable gadget is present on the blog **CVE ID : CVE-2023-4643**	N/A	A-SHO-ENAB-241123/1476
Vendor: silabs					
Product: emberznet_sdk					
Affected Version(s): * Up to (including) 7.3.1.0					
Missing Encryption of Sensitive Data	26-Oct-2023	6.1	Missing Encryption of Security Keys vulnerability in Silicon Labs Ember ZNet SDK on 32 bit, ARM (SecureVault High modules) allows potential modification or extraction of network credentials stored in flash. This issue affects Silicon Labs Ember ZNet SDK: 7.3.1 and earlier.	N/A	A-SIL-EMBE-241123/1477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-41096		
Product: gecko_bootloader					
Affected Version(s): * Up to (including) 4.3.1					
Integer Overflow or Wraparound	20-Oct-2023	7.8	An integer overflow in Silicon Labs Gecko Bootloader version 4.3.1 and earlier allows unbounded memory access when reading from or writing to storage slots. **CVE ID : CVE-2023-3487**	N/A	A-SIL-GECK-241123/1478
Product: openthread_sdk					
Affected Version(s): * Up to (including) 2.3.1.0					
Missing Encryption of Sensitive Data	26-Oct-2023	9.1	Missing Encryption of Security Keys vulnerability in Silicon Labs OpenThread SDK on 32 bit, ARM (SecureVault High modules) allows potential modification or extraction of network credentials stored in flash. This issue affects Silicon Labs	N/A	A-SIL-OPEN-241123/1479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OpenThread SDK: 2.3.1 and earlier. **CVE ID : CVE-2023-41095**		
Vendor: Silverstripe					
Product: graphql					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.8.2					
Uncontrolled Resource Consumption	16-Oct-2023	7.5	silverstripe-graphql is a package which serves Silverstripe data in GraphQL representations. An attacker could use a recursive graphql query to execute a Distributed Denial of Service attack (DDOS attack) against a website. This mostly affects websites with publicly exposed graphql schemas. If your Silverstripe CMS project does not expose a public facing graphql schema, a user account is required to trigger the DDOS attack. If your site is hosted behind a content delivery network (CDN), such as Imperva or CloudFlare, this may further mitigate the risk.	https://github.com/silverstripe/silverstripe-graphql/commit/f6d5976ec4608e51184b0db1ee5b9e9a99d2501c, https://www.silverstripe.org/download/security-releases/CVE-2023-40180	A-SIL-GRAP-241123/1480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue has been addressed in versions 3.8.2, 4.1.3, 4.2.5, 4.3.4, and 5.0.3. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-40180**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.1.3					
Uncontrolled Resource Consumption	16-Oct-2023	7.5	silverstripe-graphql is a package which serves Silverstripe data in GraphQL representations. An attacker could use a recursive graphql query to execute a Distributed Denial of Service attack (DDOS attack) against a website. This mostly affects websites with publicly exposed graphql schemas. If your Silverstripe CMS project does not expose a public facing graphql schema, a user account is required to trigger the DDOS attack. If your site is hosted behind a content delivery network (CDN), such as Imperva or	https://github.com/silverstripe/silverstripe-graphql/commit/f6d5976ec4608e51184b0db1ee5b9e9a99d2501c, https://www.silverstripe.org/download/security-releases/CVE-2023-40180	A-SIL-GRAP-241123/1481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CloudFlare, this may further mitigate the risk. This issue has been addressed in versions 3.8.2, 4.1.3, 4.2.5, 4.3.4, and 5.0.3. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-40180**		
Affected Version(s): From (including) 4.2.0 Up to (excluding) 4.2.5					
Uncontrolled Resource Consumption	16-Oct-2023	7.5	silverstripe-graphql is a package which serves Silverstripe data in GraphQL representations. An attacker could use a recursive graphql query to execute a Distributed Denial of Service attack (DDOS attack) against a website. This mostly affects websites with publicly exposed graphql schemas. If your Silverstripe CMS project does not expose a public facing graphql schema, a user account is required to trigger the DDOS attack. If your site is hosted behind a	https://github.com/silverstripe/silverstripe-graphql/commit/f6d5976ec4608e51184b0db1ee5b9e9a99d2501c, https://www.silverstripe.org/download/security-releases/CVE-2023-40180	A-SIL-GRAP-241123/1482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			content delivery network (CDN), such as Imperva or CloudFlare, this may further mitigate the risk. This issue has been addressed in versions 3.8.2, 4.1.3, 4.2.5, 4.3.4, and 5.0.3. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-40180**		
Affected Version(s): From (including) 4.3.0 Up to (excluding) 4.3.4					
Uncontrolled Resource Consumption	16-Oct-2023	7.5	silverstripe-graphql is a package which serves Silverstripe data in GraphQL representations. An attacker could use a recursive graphql query to execute a Distributed Denial of Service attack (DDOS attack) against a website. This mostly affects websites with publicly exposed graphql schemas. If your Silverstripe CMS project does not expose a public facing graphql schema, a user account is required	https://github.com/silverstripe/silverstripe-graphql/commit/f6d5976ec4608e51184b0db1ee5b9e9a99d2501c, https://www.silverstripe.org/download/security-releases/CVE-2023-40180	A-SIL-GRAP-241123/1483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to trigger the DDOS attack. If your site is hosted behind a content delivery network (CDN), such as Imperva or CloudFlare, this may further mitigate the risk. This issue has been addressed in versions 3.8.2, 4.1.3, 4.2.5, 4.3.4, and 5.0.3. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-40180**		
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.0.3					
Uncontrolled Resource Consumption	16-Oct-2023	7.5	silverstripe-graphql is a package which serves Silverstripe data in GraphQL representations. An attacker could use a recursive graphql query to execute a Distributed Denial of Service attack (DDOS attack) against a website. This mostly affects websites with publicly exposed graphql schemas. If your Silverstripe CMS project does not expose a public	https://github.com/silverstripe/silverstripe-graphql/commit/f6d5976ec4608e51184b0db1ee5b9e9a99d2501c, https://www.silverstripe.org/download/security-releases/CVE-2023-40180	A-SIL-GRAP-241123/1484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			facing graphql schema, a user account is required to trigger the DDOS attack. If your site is hosted behind a content delivery network (CDN), such as Imperva or CloudFlare, this may further mitigate the risk. This issue has been addressed in versions 3.8.2, 4.1.3, 4.2.5, 4.3.4, and 5.0.3. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-40180**		
Vendor: simplefilelist					
Product: simple_file_list					
Affected Version(s): * Up to (including) 6.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Mitchell Bennis Simple File List plugin <= 6.1.9 versions. **CVE ID : CVE-2023-39924**	N/A	A-SIM-SIMP-241123/1485
Vendor: simple_real_estate_portal_system_project					
Product: simple_real_estate_portal_system					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	26-Oct-2023	9.8	A vulnerability was found in SourceCodester Simple Real Estate Portal System 1.0. It has been classified as critical. Affected is an unknown function of the file view_estate.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-243618 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-5805**	N/A	A-SIM-SIMP-241123/1486
Vendor: simple_shortcodes_project					
Product: simple_shortcodes					
Affected Version(s): * Up to (including) 1.0.20					
N/A	30-Oct-2023	5.4	The Simple Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 1.0.20 due to insufficient input sanitization and output	N/A	A-SIM-SIMP-241123/1487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5566**		
Vendor: sisqualwfm					
Product: sisqualwfm					
Affected Version(s): From (including) 7.1.319.103 Up to (excluding) 7.1.319.111					
URL Redirection to Untrusted Site ('Open Redirect')	25-Oct-2023	6.1	The sisqualWFM 7.1.319.103 thru 7.1.319.111 for Android, has a host header injection vulnerability in its "/sisqualIdentityServer/core/" endpoint. By modifying the HTTP Host header, an attacker can change webpage links and even redirect users to arbitrary or malicious locations. This can lead to phishing attacks, malware distribution, and unauthorized	N/A	A-SIS-SISQ-241123/1488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to sensitive resources. **CVE ID : CVE-2023-36085**		
Vendor: sitekit_project					
Product: sitekit					
Affected Version(s): * Up to (including) 1.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	The Sitekit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'sitekit_iframe' shortcode in versions up to, and including, 1.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5071**	https://plugins.trac.wordpress.org/changeset/2970788/sitekit, https://plugins.trac.wordpress.org/browser/sitekit/trunk/inc/sitekit-shortcode-iframe.php#L3	A-SIT-SITE-241123/1489
Vendor: sitolog					
Product: sitolog_application_connect					
Affected Version(s): * Up to (including) 7.8.a					
Improper Neutralization of Special Elements	20-Oct-2023	9.8	Sitolog sitologapplicationconnect v7.8.a and before was discovered to	N/A	A-SIT-SITO-241123/1490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			contain a SQL injection vulnerability via the component /activate_hook.php . **CVE ID : CVE-2023-37824**		
Vendor: six2dez					
Product: reconftw					
Affected Version(s): * Up to (excluding) 2.7.1.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Oct-2023	8.8	reconFTW is a tool designed to perform automated recon on a target domain by running the best set of tools to perform scanning and finding out vulnerabilities. A vulnerability has been identified in reconftw where inadequate validation of retrieved subdomains may lead to a Remote Code Execution (RCE) attack. An attacker can exploit this vulnerability by crafting a malicious CSP entry on it's own domain. Successful exploitation can lead to the execution of arbitrary code	https://github.com/six2dez/reconftw/commit/e639de356c0880fe5fe01a32de9d0c58afb5f086, https://github.com/six2dez/reconftw/security/advisories/GHSA-fxwr-vr9x-wvjp	A-SIX-RECO-241123/1491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			within the context of the application, potentially compromising the system. This issue has been addressed in version 2.7.1.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-46117**		
Vendor: Slims					
Product: senayan_library_management_system					
Affected Version(s): 9.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	31-Oct-2023	8.8	SQL injection vulnerability in Senayan Library Management Systems Slims v.9 and Bulian v.9.6.1 allows a remote attacker to obtain sensitive information and execute arbitrary code via a crafted script to the reborrowLimit parameter in the member_type.php. **CVE ID : CVE-2023-45996**	https://github.com/slims/slims9_bulian/issues/216	A-SLI-SENA-241123/1492
Product: senayan_library_management_system_bulian					
Affected Version(s): 9.6.1					
Improper Neutralizat	31-Oct-2023	8.8	SQL injection vulnerability in	https://github.com/slims/slims	A-SLI-SENA-241123/1493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			Senayan Library Management Systems Slims v.9 and Bulian v.9.6.1 allows a remote attacker to obtain sensitive information and execute arbitrary code via a crafted script to the reborrowLimit parameter in the member_type.php. **CVE ID : CVE-2023-45996**	9_bulian/issues/216	
Vendor: small_crm_project					
Product: small_crm					
Affected Version(s): 3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	5.4	Stored Cross-Site Scripting (XSS) vulnerability in the Company field in the "Request a Quote" Section of Small CRM v3.0 allows an attacker to store and execute malicious javascript code in the Admin panel which leads to Admin account takeover. **CVE ID : CVE-2023-45394**	https://github.com/kartik753/CVE/blob/main/CVE-2023-45394	A-SMA-SMAL-241123/1494
Vendor: snegurka					
Product: referralbyphone					
Affected Version(s): * Up to (including) 3.5.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	9.8	In the module "Referral and Affiliation Program" (referralbyphone) version 3.5.1 and before from Snegurka for PrestaShop, a guest can perform SQL injection. Method `ReferralByPhoneDefaultModuleFrontController::ajaxProcessCartRuleValidate` has sensitive SQL calls that can be executed with a trivial http call and exploited to forge a SQL injection. **CVE ID : CVE-2023-46358**	N/A	A-SNE-REFE-241123/1495
Vendor: soisy					
Product: soisy_pagamento_rateale					
Affected Version(s): * Up to (including) 6.0.1					
Missing Authorization	21-Oct-2023	7.5	The Soisy Pagamento Rateale plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the parseRemoteRequest function in versions up to, and including, 6.0.1. This makes it possible for	N/A	A-SOI-SOIS-241123/1496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attackers with knowledge of an existing WooCommerce Order ID to expose sensitive WooCommerce order information (e.g., Name, Address, Email Address, and other order metadata). **CVE ID : CVE-2023-5132**		
Vendor: Solarwinds					
Product: access_rights_manager					
Affected Version(s): * Up to (including) 2023.2.0.73					
Deserialization of Untrusted Data	19-Oct-2023	9.8	The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability can be abused by unauthenticated users on SolarWinds ARM Server. **CVE ID : CVE-2023-35182**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2023-35182, https://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2023-2-1_release_notes.htm	A-SOL-ACCE-241123/1497
Deserialization of Untrusted Data	19-Oct-2023	9.8	The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an	https://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2023-2-1_release_notes.htm,	A-SOL-ACCE-241123/1498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user to abuse a SolarWinds service resulting in a remote code execution. **CVE ID : CVE-2023-35184**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2023-35184	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Oct-2023	9.8	The SolarWinds Access Rights Manager was susceptible to a Directory Traversal Remote Code Vulnerability. This vulnerability allows an unauthenticated user to achieve the Remote Code Execution. **CVE ID : CVE-2023-35187**	https://https://www.solarwinds.com/trust-center/security-advisories/CVE-2023-35187, https://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2023-2-1_release_notes.htm	A-SOL-ACCE-241123/1499
Deserialization of Untrusted Data	19-Oct-2023	8.8	The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows authenticated users to abuse SolarWinds ARM API. **CVE ID : CVE-2023-35180**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2023-35180, https://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2023-2-1_release_notes.htm	A-SOL-ACCE-241123/1500
Deserialization of Untrusted Data	19-Oct-2023	8.8	The SolarWinds Access Rights Manager was susceptible to	https://documentation.solarwinds.com/en/success_center/ar	A-SOL-ACCE-241123/1501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability. This vulnerability allows an authenticated user to abuse SolarWinds service resulting in remote code execution. **CVE ID : CVE-2023-35186**	m/content/release_notes/arm_2023-2-1_release_notes.htm, https://www.solarwinds.com/trust-center/security-advisories/CVE-2023-35186	
Incorrect Default Permissions	19-Oct-2023	7.8	The SolarWinds Access Rights Manager was susceptible to Privilege Escalation Vulnerability. This vulnerability allows users to abuse incorrect folder permission resulting in Privilege Escalation. **CVE ID : CVE-2023-35181**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2023-35181	A-SOL-ACCE-241123/1502
Incorrect Default Permissions	19-Oct-2023	7.8	The SolarWinds Access Rights Manager was susceptible to Privilege Escalation Vulnerability. This vulnerability allows authenticated users to abuse local resources to Privilege Escalation.	https://www.solarwinds.com/trust-center/security-advisories/CVE-2023-35183, https://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2023-2-	A-SOL-ACCE-241123/1503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35183	1_release_notes.htm	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Oct-2023	7.2	The SolarWinds Access Rights Manager was susceptible to a Directory Traversal Remote Code Vulnerability using SYSTEM privileges. **CVE ID : CVE-2023-35185**	https://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2023-2-1_release_notes.htm, https://www.solarwinds.com/trust-center/security-advisories/CVE-2023-35185	A-SOL-ACCE-241123/1504
Vendor: sollace					
Product: unicopia					
Affected Version(s): * Up to (excluding) 1.2.0					
Deserialization of Untrusted Data	20-Oct-2023	9.8	Sollace Unicopia version 1.1.1 and before was discovered to deserialize untrusted data, allowing attackers to execute arbitrary code. **CVE ID : CVE-2023-39680**	N/A	A-SOL-UNIC-241123/1505
Vendor: solwininfotech					
Product: user_activity_log					
Affected Version(s): * Up to (excluding) 2.3.4					
N/A	16-Oct-2023	7.5	This user-activity-log-pro WordPress plugin before 2.3.4 retrieves client IP addresses from potentially	N/A	A-SOL-USER-241123/1506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			untrusted headers, allowing an attacker to manipulate its value. This may be used to hide the source of malicious traffic. **CVE ID : CVE-2023-5133**		
N/A	16-Oct-2023	5.4	The User Activity Log Pro WordPress plugin before 2.3.4 does not properly escape recorded User-Agents in the user activity logs dashboard, which may allow visitors to conduct Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-5167**	N/A	A-SOL-USER-241123/1507
Vendor: Sonicwall					
Product: directory_services_connector					
Affected Version(s): * Up to (excluding) 4.1.22					
Improper Privilege Management	27-Oct-2023	7.8	A local privilege escalation vulnerability in SonicWall Directory Services Connector Windows MSI client 4.1.21 and earlier versions allows a local low-privileged user to gain system privileges through	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0016	A-SON-DIRE-241123/1508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running the recovery feature. **CVE ID : CVE-2023-44219**		
Product: netextender					
Affected Version(s): * Up to (including) 10.2.336					
Uncontrolled Search Path Element	27-Oct-2023	7.3	SonicWall NetExtender Windows (32-bit and 64-bit) client 10.2.336 and earlier versions have a DLL Search Order Hijacking vulnerability in the start-up DLL component. Successful exploitation via a local attacker could result in command execution in the target system. **CVE ID : CVE-2023-44220**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0017	A-SON-NETE-241123/1509
Vendor: Sophos					
Product: firewall					
Affected Version(s): * Up to (including) 19.5.3					
Insufficiently Protected Credentials	18-Oct-2023	7.5	A password disclosure vulnerability in the Secure PDF eXchange (SPX) feature allows attackers with full email access to decrypt PDFs in Sophos Firewall version 19.5 MR3 (19.5.3) and older, if the password	https://www.sophos.com/en-us/security-advisories/sophos-sa-20231017-spx-password	A-SOP-FIRE-241123/1510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			type is set to "Specified by sender". **CVE ID : CVE-2023-5552**		
Vendor: Southrivertech					
Product: titan_ftp_server					
Affected Version(s): * Up to (including) 2.0.16.2277					
Incorrect Default Permissions	16-Oct-2023	4.9	Default file permissions on South River Technologies' Titan MFT and Titan SFTP servers on Linux allows a user that's authentication to the OS to read sensitive files on the filesystem **CVE ID : CVE-2023-45690**	https://helpdesk.southrivertech.com/portal/en/kb/articles/security-patch-for-issues-cve-2023-45685-through-cve-2023-45690	A-SOU-TITA-241123/1511
Product: titan_mfp_server					
Affected Version(s): * Up to (excluding) 2.0.18					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Oct-2023	7.2	Insufficient path validation when writing a file via WebDAV in South River Technologies' Titan MFT and Titan SFTP servers on Linux allows an authenticated attacker to write a file to any location on the filesystem via path traversal **CVE ID : CVE-2023-45686**	https://helpdesk.southrivertech.com/portal/en/kb/articles/security-patch-for-issues-cve-2023-45685-through-cve-2023-45690	A-SOU-TITA-241123/1512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: titan_mft_server					
Affected Version(s): * Up to (excluding) 2.0.18					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Oct-2023	9.1	Insufficient path validation when extracting a zip archive in South River Technologies' Titan MFT and Titan SFTP servers on Windows and Linux allows an authenticated attacker to write a file to any location on the filesystem via path traversal **CVE ID : CVE-2023-45685**	https://helpdesk.southrivertech.com/portal/en/kb/articles/security-patch-for-issues-cve-2023-45685-through-cve-2023-45690	A-SOU-TITA-241123/1513
Session Fixation	16-Oct-2023	8.8	A session fixation vulnerability in South River Technologies' Titan MFT and Titan SFTP servers on Linux and Windows allows an attacker to bypass the server's authentication if they can trick an administrator into authorizating a session id of their choosing **CVE ID : CVE-2023-45687**	https://helpdesk.southrivertech.com/portal/en/kb/articles/security-patch-for-issues-cve-2023-45685-through-cve-2023-45690	A-SOU-TITA-241123/1514
Improper Limitation of a Pathname to a	16-Oct-2023	6.5	Lack of sufficient path validation in South River Technologies' Titan MFT and Titan	https://helpdesk.southrivertech.com/portal/en/kb/articles/security-patch-	A-SOU-TITA-241123/1515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			SFTP servers on Windows and Linux allows an authenticated attacker with administrative privileges to read any file on the filesystem via path traversal **CVE ID : CVE-2023-45689**	for-issues-cve-2023-45685-through-cve-2023-45690	
Incorrect Default Permissions	16-Oct-2023	4.9	Default file permissions on South River Technologies' Titan MFT and Titan SFTP servers on Linux allows a user that's authentication to the OS to read sensitive files on the filesystem **CVE ID : CVE-2023-45690**	https://helpdesk.southrivertech.com/portal/en/kb/articles/security-patch-for-issues-cve-2023-45685-through-cve-2023-45690	A-SOU-TITA-241123/1516
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Oct-2023	4.3	Lack of sufficient path validation in South River Technologies' Titan MFT and Titan SFTP servers on Linux allows an authenticated attacker to get the size of an arbitrary file on the filesystem using path traversal in the ftp "SIZE" command	https://helpdesk.southrivertech.com/portal/en/kb/articles/security-patch-for-issues-cve-2023-45685-through-cve-2023-45690	A-SOU-TITA-241123/1517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45688		
Product: titan_sftp_server					
Affected Version(s): * Up to (excluding) 2.0.18					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Oct-2023	9.1	Insufficient path validation when extracting a zip archive in South River Technologies' Titan MFT and Titan SFTP servers on Windows and Linux allows an authenticated attacker to write a file to any location on the filesystem via path traversal **CVE ID : CVE-2023-45685**	https://helpdesk.southrivertech.com/portal/en/kb/articles/security-patch-for-issues-cve-2023-45685-through-cve-2023-45690	A-SOU-TITA-241123/1518
Session Fixation	16-Oct-2023	8.8	A session fixation vulnerability in South River Technologies' Titan MFT and Titan SFTP servers on Linux and Windows allows an attacker to bypass the server's authentication if they can trick an administrator into authorizating a session id of their choosing **CVE ID : CVE-2023-45687**	https://helpdesk.southrivertech.com/portal/en/kb/articles/security-patch-for-issues-cve-2023-45685-through-cve-2023-45690	A-SOU-TITA-241123/1519
Improper Limitation of a	16-Oct-2023	6.5	Lack of sufficient path validation in South River	https://helpdesk.southrivertech.com/portal/e	A-SOU-TITA-241123/1520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			Technologies' Titan MFT and Titan SFTP servers on Windows and Linux allows an authenticated attacker with administrative privileges to read any file on the filesystem via path traversal **CVE ID : CVE-2023-45689**	n/kb/articles/security-patch-for-issues-cve-2023-45685-through-cve-2023-45690	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Oct-2023	4.3	Lack of sufficient path validation in South River Technologies' Titan MFT and Titan SFTP servers on Linux allows an authenticated attacker to get the size of an arbitrary file on the filesystem using path traversal in the ftp "SIZE" command **CVE ID : CVE-2023-45688**	https://helpdesk.southrivertech.com/portal/en/kb/articles/security-patch-for-issues-cve-2023-45685-through-cve-2023-45690	A-SOU-TITA-241123/1521
Vendor: spaceapplications					
Product: yamcs					
Affected Version(s): 5.8.6					
Improper Limitation of a Pathname to a Restricted Directory	19-Oct-2023	9.1	Directory Traversal vulnerability in the storage functionality of the API in Yamcs 5.8.6 allows attackers to delete arbitrary files via crafted	https://github.com/yamcs/yamcs/compare/yamcs-5.8.6...yamcs-5.8.7	A-SPA-YAMC-241123/1522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			HTTP DELETE request. **CVE ID : CVE-2023-45278**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Oct-2023	7.5	Yamcs 5.8.6 is vulnerable to directory traversal (issue 1 of 2). The vulnerability is in the storage functionality of the API and allows one to escape the base directory of the buckets, freely navigate system directories, and read arbitrary files. **CVE ID : CVE-2023-45277**	https://github.com/yamcs/yamcs/compare/yamcs-5.8.6...yamcs-5.8.7	A-SPA-YAMC-241123/1523
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2023	6.1	An issue in Yamcs 5.8.6 allows attackers to obtain the session cookie via upload of crafted HTML file. **CVE ID : CVE-2023-45281**	N/A	A-SPA-YAMC-241123/1524
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2023	5.4	Yamcs 5.8.6 allows XSS (issue 1 of 2). It comes with a Bucket as its primary storage mechanism. Buckets allow for the upload of any file. There's a way to upload a display referencing a malicious JavaScript file to	https://github.com/yamcs/yamcs/compare/yamcs-5.8.6...yamcs-5.8.7	A-SPA-YAMC-241123/1525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the bucket. The user can then open the uploaded display by selecting Telemetry from the menu and navigating to the display. **CVE ID : CVE-2023-45279**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2023	5.4	Yamcs 5.8.6 allows XSS (issue 2 of 2). It comes with a Bucket as its primary storage mechanism. Buckets allow for the upload of any file. There's a way to upload an HTML file containing arbitrary JavaScript and then navigate to it. Once the user opens the file, the browser will execute the arbitrary JavaScript. **CVE ID : CVE-2023-45280**	https://github.com/yamcs/yamcs/compare/yamcs-5.8.6...yamcs-5.8.7	A-SPA-YAMC-241123/1526
Vendor: spiderteams					
Product: applyonline_-_application_form_builder_and_manager					
Affected Version(s): * Up to (including) 2.5.2					
Improper Neutralization of Input During Web Page Generation	25-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Spider Teams ApplyOnline – Application Form Builder and	N/A	A-SPI-APPL-241123/1527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Manager plugin <= 2.5.2 versions. **CVE ID : CVE-2023-45756**		
Vendor: stellar					
Product: rs-stellar-strkey					
Affected Version(s): * Up to (excluding) 0.0.8					
N/A	25-Oct-2023	7.5	rs-stellar-strkey is a Rust lib for encode/decode of Stellar Strkeys. A panic vulnerability occurs when a specially crafted payload is used.`inner_payload_len` should not above 64. This vulnerability has been patched in version 0.0.8. **CVE ID : CVE-2023-46135**	https://github.com/stellar/rs-stellar-strkey/security/advisories/GHSA-5873-6fwq-463f	A-STE-RS-S-241123/1528
Vendor: stephanieleary					
Product: next_page					
Affected Version(s): * Up to (including) 1.5.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Stephanie Leary Next Page plugin <= 1.5.2 versions. **CVE ID : CVE-2023-45768**	N/A	A-STE-NEXT-241123/1529
Vendor: stylemixthemes					
Product: motors_-_car_dealer\,_classifieds_\&_listing					
Affected Version(s): * Up to (including) 1.4.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in StylemixThemes Motors – Car Dealer, Classifieds & Listing plugin <= 1.4.6 versions. **CVE ID : CVE-2023-46208**	N/A	A-STY-MOTO-241123/1530
Vendor: Sugarcrm					
Product: sugarcrm					
Affected Version(s): 13.0.0					
Unrestricted Upload of File with Dangerous Type	27-Oct-2023	8.8	An issue was discovered in SugarCRM 12 before 12.0.4 and 13 before 13.0.2. An Unrestricted File Upload vulnerability has been identified in the Notes module. By using a crafted request, custom PHP code can be injected via the Notes module because of missing input validation. An attacker with regular user privileges can exploit this. **CVE ID : CVE-2023-46815**	https://support.sugarcrm.com/resources/security/sugarcrm-sa-2023-011/	A-SUG-SUGA-241123/1531
Improper Control of Generation of Code	27-Oct-2023	8.8	An issue was discovered in SugarCRM 12 before 12.0.4 and 13 before 13.0.2. A Server Site	https://support.sugarcrm.com/resources/security/sugarcrm-sa-2023-010/	A-SUG-SUGA-241123/1532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			Template Injection (SSTI) vulnerability has been identified in the GecControl action. By using a crafted request, custom PHP code can be injected via the GetControl action because of missing input validation. An attacker with regular user privileges can exploit this. **CVE ID : CVE-2023-46816**		
Affected Version(s): 13.0.1					
Unrestricted Upload of File with Dangerous Type	27-Oct-2023	8.8	An issue was discovered in SugarCRM 12 before 12.0.4 and 13 before 13.0.2. An Unrestricted File Upload vulnerability has been identified in the Notes module. By using a crafted request, custom PHP code can be injected via the Notes module because of missing input validation. An attacker with regular user privileges can exploit this. **CVE ID : CVE-2023-46815**	https://support.sugarcrm.com/resources/security/sugarcrm-sa-2023-011/	A-SUG-SUGA-241123/1533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	27-Oct-2023	8.8	An issue was discovered in SugarCRM 12 before 12.0.4 and 13 before 13.0.2. A Server Site Template Injection (SSTI) vulnerability has been identified in the GecControl action. By using a crafted request, custom PHP code can be injected via the GetControl action because of missing input validation. An attacker with regular user privileges can exploit this. **CVE ID : CVE-2023-46816**	https://support.sugarcrm.com/resources/security/sugarcrm-sa-2023-010/	A-SUG-SUGA-241123/1534
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.0.4					
Unrestricted Upload of File with Dangerous Type	27-Oct-2023	8.8	An issue was discovered in SugarCRM 12 before 12.0.4 and 13 before 13.0.2. An Unrestricted File Upload vulnerability has been identified in the Notes module. By using a crafted request, custom PHP code can be injected via the Notes module because of missing input validation. An attacker with	https://support.sugarcrm.com/resources/security/sugarcrm-sa-2023-011/	A-SUG-SUGA-241123/1535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			regular user privileges can exploit this. **CVE ID : CVE-2023-46815**		
Improper Control of Generation of Code ('Code Injection')	27-Oct-2023	8.8	An issue was discovered in SugarCRM 12 before 12.0.4 and 13 before 13.0.2. A Server Site Template Injection (SSTI) vulnerability has been identified in the GecControl action. By using a crafted request, custom PHP code can be injected via the GetControl action because of missing input validation. An attacker with regular user privileges can exploit this. **CVE ID : CVE-2023-46816**	https://support.sugarcrm.com/resources/security/sugarcrm-sa-2023-010/	A-SUG-SUGA-241123/1536
Vendor: Superwebmailer					
Product: superwebmailer					
Affected Version(s): 9.00.0.01710					
Improper Neutralization of Special Elements used in an SQL Command	21-Oct-2023	8.8	An issue was discovered in SuperWebMailer 9.00.0.01710. It allows Export SQL Injection via the size parameter. **CVE ID : CVE-2023-38190**	N/A	A-SUP-SUPE-241123/1537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	21-Oct-2023	8.8	An issue was discovered in SuperWebMailer 9.00.0.01710. It allows Remote Code Execution via a crafted sendmail command line. **CVE ID : CVE-2023-38193**	N/A	A-SUP-SUPE-241123/1538
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	6.1	An issue was discovered in SuperWebMailer 9.00.0.01710. It allows spamtest_external.php XSS via a crafted filename. **CVE ID : CVE-2023-38191**	N/A	A-SUP-SUPE-241123/1539
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-2023	6.1	An issue was discovered in SuperWebMailer 9.00.0.01710. It allows superadmincreate.php XSS via crafted incorrect passwords. **CVE ID : CVE-2023-38192**	N/A	A-SUP-SUPE-241123/1540
Improper Neutralization of Input During Web Page Generation	21-Oct-2023	6.1	An issue was discovered in SuperWebMailer 9.00.0.01710. It allows keepalive.php XSS via a GET parameter.	N/A	A-SUP-SUPE-241123/1541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-38194**		
Vendor: syedbalkhi					
Product: wp_lightbox_2					
Affected Version(s): * Up to (including) 3.0.6.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Syed Balkhi WP Lightbox 2 plugin <= 3.0.6.5 versions. **CVE ID : CVE-2023-45747**	N/A	A-SYE-WP_L-241123/1542
Vendor: taggbox					
Product: taggbox					
Affected Version(s): * Up to (including) 2.9					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Taggbox plugin <= 2.9 versions. **CVE ID : CVE-2023-45763**	N/A	A-TAG-TAGG-241123/1543
Vendor: tammersoft					
Product: shared_files					
Affected Version(s): * Up to (excluding) 1.7.6					
N/A	16-Oct-2023	6.1	The Shared Files WordPress plugin before 1.7.6 does not return the right Content-Type header for the specified uploaded file. Therefore, an attacker can upload an allowed file extension	N/A	A-TAM-SHAR-241123/1544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injected with malicious scripts. **CVE ID : CVE-2023-4819**		
Vendor: task_reminder_system_project					
Product: task_reminder_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Oct-2023	9.8	A vulnerability was found in SourceCodester Task Reminder System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file classes/Users.php?f=delete. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The identifier of this vulnerability is VDB-243800. **CVE ID : CVE-2023-5836**	N/A	A-TAS-TASK-241123/1545
Vendor: tauri					
Product: tauri					
Affected Version(s): * Up to (excluding) 2.0.0					
Insufficiently Protected Credentials	20-Oct-2023	5.5	Tauri is a framework for building binaries for all major desktop platforms. This advisory is not describing a vulnerability in the	https://github.com/tauri-apps/tauri/security/advisories/GHSA-2rcp-jvr4-r259	A-TAU-TAUR-241123/1546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Tauri code base itself but a commonly used misconfiguration which could lead to leaking of the private key and updater key password into bundled Tauri applications using the Vite frontend in a specific configuration. The Tauri documentation used an insecure example configuration in the `Vite guide` to showcase how to use Tauri together with Vite. Copying the following snippet `envPrefix: ['VITE_', 'TAURI_'],` from this guide into the `vite.config.ts` of a Tauri project leads to bundling the `TAURI_PRIVATE_KEY` and `TAURI_KEY_PASSWORD` into the Vite frontend code and therefore leaking this value to the released Tauri application. Using the `envPrefix: ['VITE_'],` or any other framework		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than Vite means you are not impacted by this advisory. Users are advised to rotate their updater private key if they are affected by this (requires Tauri CLI >=1.5.5). After updating the envPrefix configuration, generate a new private key with `tauri signer generate`, saving the new private key and updating the updater's `pubkey` value on `tauri.conf.json` with the new public key. To update your existing application, the next application build must be signed with the older private key in order to be accepted by the existing application. **CVE ID : CVE-2023-46115**		
Affected Version(s): 2.0.0					
Insufficiently Protected Credentials	20-Oct-2023	5.5	Tauri is a framework for building binaries for all major desktop platforms.	https://github.com/tauri-apps/tauri/security/advisories/	A-TAU-TAUR-241123/1547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This advisory is not describing a vulnerability in the Tauri code base itself but a commonly used misconfiguration which could lead to leaking of the private key and updater key password into bundled Tauri applications using the Vite frontend in a specific configuration. The Tauri documentation used an insecure example configuration in the `Vite guide` to showcase how to use Tauri together with Vite. Copying the following snippet `envPrefix: ['VITE_', 'TAURI_'],` from this guide into the `vite.config.ts` of a Tauri project leads to bundling the `TAURI_PRIVATE_KEY` and `TAURI_KEY_PASSWORD` into the Vite frontend code and therefore leaking this value to the released Tauri application. Using the	GHSA-2rcp-jvr4-r259	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`envPrefix: ['VITE_'],` or any other framework than Vite means you are not impacted by this advisory. Users are advised to rotate their updater private key if they are affected by this (requires Tauri CLI >=1.5.5). After updating the envPrefix configuration, generate a new private key with `tauri signer generate`, saving the new private key and updating the updater's `pubkey` value on `tauri.conf.json` with the new public key. To update your existing application, the next application build must be signed with the older private key in order to be accepted by the existing application. **CVE ID : CVE-2023-46115**		
Vendor: technowich					
Product: wp_ulike_-_most_advanced_wordpress_marketing_toolkit					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 4.6.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in TechnoWich WP ULike – Most Advanced WordPress Marketing Toolkit plugin <= 4.6.8 versions. **CVE ID : CVE-2023-45640**	N/A	A-TEC-WP_U-241123/1548
Vendor: Tenable					
Product: nessus_network_monitor					
Affected Version(s): * Up to (excluding) 6.3.0					
Improper Privilege Management	26-Oct-2023	8.8	Under certain conditions, Nessus Network Monitor could allow a low privileged user to escalate privileges to NT AUTHORITY\SYSTEM on Windows hosts by replacing a specially crafted file. **CVE ID : CVE-2023-5622**	https://www.tenable.com/security/tns-2023-34	A-TEN-NESS-241123/1549
Improper Control of Generation of Code ('Code Injection')	26-Oct-2023	7.8	NNM failed to properly set ACLs on its installation directory, which could allow a low privileged user to run arbitrary code	https://www.tenable.com/security/tns-2023-34	A-TEN-NESS-241123/1550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with SYSTEM privileges where NNM is installed to a non-standard location **CVE ID : CVE-2023-5623**		
Improper Input Validation	26-Oct-2023	7.2	Under certain conditions, Nessus Network Monitor was found to not properly enforce input validation. This could allow an admin user to alter parameters that could potentially allow a blindSQL injection. **CVE ID : CVE-2023-5624**	https://www.tenable.com/security/tns-2023-34	A-TEN-NESS-241123/1551
Vendor: teomantuncer					
Product: node_email_check					
Affected Version(s): 1.0.4					
N/A	25-Oct-2023	7.5	ReDos in NPMJS Node Email Check v.1.0.4 allows an attacker to cause a denial of service via a crafted string to the scpSyntax component. **CVE ID : CVE-2023-39619**	N/A	A-TEO-NODE-241123/1552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: terminalfour					
Product: terminalfour					
Affected Version(s): 7.4.0004					
Incorrect Authorization	16-Oct-2023	6.5	In Terminalfour before 8.3.16, misconfigured LDAP users are able to login with an invalid password. **CVE ID : CVE-2023-29484**	https://docs.terminalfour.com/articles/security-notices/cve-2023-29484/	A-TER-TERM-241123/1553
Affected Version(s): 8.2.18.2.3					
Incorrect Authorization	16-Oct-2023	6.5	In Terminalfour before 8.3.16, misconfigured LDAP users are able to login with an invalid password. **CVE ID : CVE-2023-29484**	https://docs.terminalfour.com/articles/security-notices/cve-2023-29484/	A-TER-TERM-241123/1554
Affected Version(s): 8.2.18.8					
Incorrect Authorization	16-Oct-2023	6.5	In Terminalfour before 8.3.16, misconfigured LDAP users are able to login with an invalid password. **CVE ID : CVE-2023-29484**	https://docs.terminalfour.com/articles/security-notices/cve-2023-29484/	A-TER-TERM-241123/1555
Affected Version(s): 8.3.11.2					
Incorrect Authorization	16-Oct-2023	6.5	In Terminalfour before 8.3.16, misconfigured LDAP users are able to login with an invalid password.	https://docs.terminalfour.com/articles/security-notices/cve-2023-29484/	A-TER-TERM-241123/1556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29484		
Affected Version(s): 8.3.14.2					
Incorrect Authorization	16-Oct-2023	6.5	In Terminalfour before 8.3.16, misconfigured LDAP users are able to login with an invalid password. **CVE ID : CVE-2023-29484**	https://docs.terminalfour.com/articles/security-notices/cve-2023-29484/	A-TER-TERM-241123/1557
Affected Version(s): 8.3.16					
Incorrect Authorization	16-Oct-2023	6.5	In Terminalfour before 8.3.16, misconfigured LDAP users are able to login with an invalid password. **CVE ID : CVE-2023-29484**	https://docs.terminalfour.com/articles/security-notices/cve-2023-29484/	A-TER-TERM-241123/1558
Vendor: themeblvd					
Product: tweeple					
Affected Version(s): * Up to (including) 0.9.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Theme Blvd Tweeple plugin <= 0.9.5 versions. **CVE ID : CVE-2023-30781**	N/A	A-THE-TWEE-241123/1559
Vendor: themepoints					
Product: super_testimonials					
Affected Version(s): * Up to (including) 2.9					
Improper Neutralizat	20-Oct-2023	5.4	The Super Testimonials	https://plugins.trac.wordpress.	A-THE-SUPE-241123/1560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'tpsscode' shortcode in all versions up to, and including, 2.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5613**	org/browser/super-testimonial/tags/2.8/tp-testimonials.php#L214, https://plugins.trac.wordpress.org/changeset/2979378/super-testimonial#file9	
Product: team_showcase					
Affected Version(s): * Up to (including) 2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2023	5.4	The Team Showcase plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'tmfshortcode' shortcode in all versions up to, and including, 2.1 due to insufficient	https://plugins.trac.wordpress.org/browser/team-showcase/trunk/team-manager-free.php?rev=2912143#L489, https://plugins.trac.wordpress.org/browser/te	A-THE-TEAM-251123/1561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5639**	am-showcase/trunk/team-manager-free.php?rev=2912143#L893	
Vendor: themeum					
Product: tutor_lms					
Affected Version(s): * Up to (excluding) 2.3.0					
N/A	16-Oct-2023	5.4	The Tutor LMS WordPress plugin before 2.3.0 does not sanitise and escape some of its settings, which could allow users such as subscriber to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-4805**	N/A	A-THE-TUTO-251123/1562
Vendor: themevolty					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: theme_volty_cms_blog					
Affected Version(s): * Up to (including) 4.0.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	31-Oct-2023	9.8	SQL injection vulnerability found in PrestaShop themevolty v.4.0.8 and before allow a remote attacker to gain privileges via the tvcmsblog, tvcmsvideotab, tvcmswishlist, tvcmsbrandlist, tvcmscategorychainslider, tvcmscategoryproduct, tvcmscategoryslider, tvcmspaymenticon, tvcmstestimonial components. **CVE ID : CVE-2023-27846**	https://security.friendsofpresta.org/modules/2023/10/25/tvcmsblog.html	A-THE-THEM-251123/1563
Vendor: thingnario					
Product: photon					
Affected Version(s): 1.0					
N/A	21-Oct-2023	8.8	An issue in ThingNario Photon v.1.0 allows a remote attacker to execute arbitrary code and escalate privileges via a crafted script to the ping function to the "thingnario Logger Maintenance Webpage" endpoint.	N/A	A-THI-PHOT-251123/1564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46055		
Vendor: thirtybees					
Product: thirty_bees					
Affected Version(s): 1.4.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	6.1	Thirty Bees Core v1.4.0 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the backup_pagination parameter at /controller/AdminController.php. This vulnerability allows attackers to execute arbitrary JavaScript in the web browser of a user via a crafted payload. **CVE ID : CVE-2023-45958**	https://github.com/thirtybees/thirtybees/commit/2c99464376ad7b3c95f220163a2411e35274c3ba	A-THI-THIR-251123/1565
Vendor: Tibco					
Product: hawk					
Affected Version(s): * Up to (excluding) 6.2.3					
Use of Hard-coded Credentials	25-Oct-2023	8.8	The Hawk Console and Hawk Agent components of TIBCO Software Inc.'s TIBCO Hawk, TIBCO Hawk Distribution for TIBCO Silver Fabric, TIBCO Operational Intelligence Hawk RedTail, and TIBCO Runtime Agent	https://www.tibco.com/services/support/advisories	A-TIB-HAWK-251123/1566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a vulnerability that theoretically allows an attacker with access to the Hawk Console's and Agent's log to obtain credentials used to access associated EMS servers. Affected releases are TIBCO Software Inc.'s TIBCO Hawk: versions 6.2.2 and below, TIBCO Hawk Distribution for TIBCO Silver Fabric: versions 6.2.2 and below, TIBCO Operational Intelligence Hawk RedTail: versions 7.2.1 and below, and TIBCO Runtime Agent: versions 5.12.2 and below. **CVE ID : CVE-2023-26219**		
Product: hawk_distribution_for_tibco_silver_fabric					
Affected Version(s): * Up to (excluding) 6.2.3					
Use of Hard-coded Credentials	25-Oct-2023	8.8	The Hawk Console and Hawk Agent components of TIBCO Software Inc.'s TIBCO Hawk, TIBCO Hawk Distribution for TIBCO Silver	https://www.tibco.com/services/support/advisories	A-TIB-HAWK-251123/1567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fabric, TIBCO Operational Intelligence Hawk RedTail, and TIBCO Runtime Agent contain a vulnerability that theoretically allows an attacker with access to the Hawk Console's and Agent's log to obtain credentials used to access associated EMS servers. Affected releases are TIBCO Software Inc.'s TIBCO Hawk: versions 6.2.2 and below, TIBCO Hawk Distribution for TIBCO Silver Fabric: versions 6.2.2 and below, TIBCO Operational Intelligence Hawk RedTail: versions 7.2.1 and below, and TIBCO Runtime Agent: versions 5.12.2 and below. **CVE ID : CVE-2023-26219**		
Product: operational_intelligence_hawk_redtail					
Affected Version(s): * Up to (excluding) 7.2.2					
Use of Hard-	25-Oct-2023	8.8	The Hawk Console and Hawk Agent components of	https://www.tibco.com/servic	A-TIB-OPER-251123/1568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			TIBCO Software Inc.'s TIBCO Hawk, TIBCO Hawk Distribution for TIBCO Silver Fabric, TIBCO Operational Intelligence Hawk RedTail, and TIBCO Runtime Agent contain a vulnerability that theoretically allows an attacker with access to the Hawk Console's and Agent's log to obtain credentials used to access associated EMS servers. Affected releases are TIBCO Software Inc.'s TIBCO Hawk: versions 6.2.2 and below, TIBCO Hawk Distribution for TIBCO Silver Fabric: versions 6.2.2 and below, TIBCO Operational Intelligence Hawk RedTail: versions 7.2.1 and below, and TIBCO Runtime Agent: versions 5.12.2 and below. **CVE ID : CVE-2023-26219**	es/support/advisories	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: runtime_agent					
Affected Version(s): * Up to (excluding) 5.12.3					
Use of Hard-coded Credentials	25-Oct-2023	8.8	The Hawk Console and Hawk Agent components of TIBCO Software Inc.'s TIBCO Hawk, TIBCO Hawk Distribution for TIBCO Silver Fabric, TIBCO Operational Intelligence Hawk RedTail, and TIBCO Runtime Agent contain a vulnerability that theoretically allows an attacker with access to the Hawk Console's and Agent's log to obtain credentials used to access associated EMS servers. Affected releases are TIBCO Software Inc.'s TIBCO Hawk: versions 6.2.2 and below, TIBCO Hawk Distribution for TIBCO Silver Fabric: versions 6.2.2 and below, TIBCO Operational Intelligence Hawk RedTail: versions 7.2.1 and below, and TIBCO Runtime Agent: versions 5.12.2 and below.	https://www.tibco.com/services/support/advisories	A-TIB-RUNT-251123/1569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26219		
Vendor: tiny					
Product: tinymce					
Affected Version(s): * Up to (excluding) 5.10.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2023	6.1	TinyMCE is an open source rich text editor. A mutation cross-site scripting (mXSS) vulnerability was discovered in TinyMCE's core undo and redo functionality. When a carefully-crafted HTML snippet passes the XSS sanitisation layer, it is manipulated as a string by internal trimming functions before being stored in the undo stack. If the HTML snippet is restored from the undo stack, the combination of the string manipulation and reparative parsing by either the browser's native [DOMParser API](https://developer.mozilla.org/en-US/docs/Web/API/DOMParser) (TinyMCE 6) or the	https://github.com/tinymce/tinymce/security/advisories/GHSA-v65r-p3vv-jjfv	A-TIN-TINY-251123/1570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SaxParser API (TinyMCE 5) mutates the HTML maliciously, allowing an XSS payload to be executed. This vulnerability has been patched in TinyMCE 5.10.8 and TinyMCE 6.7.1 by ensuring HTML is trimmed using node-level manipulation instead of string manipulation. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45818**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2023	6.1	TinyMCE is an open source rich text editor. A cross-site scripting (XSS) vulnerability was discovered in TinyMCE's Notification Manager API. The vulnerability exploits TinyMCE's unfiltered notification system, which is used in error handling. The conditions for this exploit requires carefully crafted malicious content	https://github.com/tinymce/tinymce/security/advisories/GHSA-hgqx-r2hp-jr38	A-TIN-TINY-251123/1571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to have been inserted into the editor and a notification to have been triggered. When a notification was opened, the HTML within the text argument was displayed unfiltered in the notification. The vulnerability allowed arbitrary JavaScript execution when an notification presented in the TinyMCE UI for the current user. This issue could also be exploited by any integration which uses a TinyMCE notification to display unfiltered HTML content. This vulnerability has been patched in TinyMCE 5.10.8 and TinyMCE 6.7.1 by ensuring that the HTML displayed in the notification is sanitized, preventing the exploit. Users are advised to upgrade. There are no known workarounds for this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45819		
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.7.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2023	6.1	TinyMCE is an open source rich text editor. A mutation cross-site scripting (mXSS) vulnerability was discovered in TinyMCE's core undo and redo functionality. When a carefully-crafted HTML snippet passes the XSS sanitisation layer, it is manipulated as a string by internal trimming functions before being stored in the undo stack. If the HTML snippet is restored from the undo stack, the combination of the string manipulation and reparative parsing by either the browser's native [DOMParser API](https://developer.mozilla.org/en-US/docs/Web/API/DOMParser) (TinyMCE 6) or the SaxParser API (TinyMCE 5) mutates the HTML maliciously,	https://github.com/tinymce/tinymce/security/advisories/GHSA-v65r-p3vv-jjfv	A-TIN-TINY-251123/1572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowing an XSS payload to be executed. This vulnerability has been patched in TinyMCE 5.10.8 and TinyMCE 6.7.1 by ensuring HTML is trimmed using node-level manipulation instead of string manipulation. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45818**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-2023	6.1	TinyMCE is an open source rich text editor. A cross-site scripting (XSS) vulnerability was discovered in TinyMCE's Notification Manager API. The vulnerability exploits TinyMCE's unfiltered notification system, which is used in error handling. The conditions for this exploit requires carefully crafted malicious content to have been inserted into the editor and a notification to have	https://github.com/tinymce/tinymce/security/advisories/GHSA-hgqx-r2hp-jr38	A-TIN-TINY-251123/1573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been triggered. When a notification was opened, the HTML within the text argument was displayed unfiltered in the notification. The vulnerability allowed arbitrary JavaScript execution when an notification presented in the TinyMCE UI for the current user. This issue could also be exploited by any integration which uses a TinyMCE notification to display unfiltered HTML content. This vulnerability has been patched in TinyMCE 5.10.8 and TinyMCE 6.7.1 by ensuring that the HTML displayed in the notification is sanitized, preventing the exploit. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45819**		
Vendor: tongda2000					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: tongda_oa					
Affected Version(s): * Up to (excluding) 11.10					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Oct-2023	9.8	A vulnerability has been found in Tongda OA 2017 and classified as critical. This vulnerability affects unknown code of the file general/hr/training/record/delete.php. The manipulation of the argument RECORD_ID leads to sql injection. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. VDB-243058 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-5682**	N/A	A-TON-TONG-251123/1574
Improper Neutralization of	26-Oct-2023	9.8	A vulnerability classified as critical was found in	N/A	A-TON-TONG-251123/1575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			Tongda OA 2017 11.10. This vulnerability affects unknown code of the file general/system/approve_center/flow_guide/flow_type/set_print/delete.php. The manipulation of the argument DELETE_STR leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-243586 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-5780**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	9.8	A vulnerability, which was classified as critical, has been found in Tongda OA 2017 11.10. This issue affects the function DELETE_STR of the file general/system/res_manage/monitor	N/A	A-TON-TONG-251123/1576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/delete_webmail.php. The manipulation 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-243587. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-5781**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	9.8	A vulnerability, which was classified as critical, was found in Tongda OA 2017 up to 11.10. Affected is an unknown function of the file /manage/delete_query.php of the component General News. The manipulation of the argument NEWS_ID leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier	N/A	A-TON-TONG-251123/1577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability is VDB-243588. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-5782**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	7.5	A vulnerability has been found in Tongda OA 2017 up to 11.9 and classified as critical. Affected by this vulnerability is an unknown functionality of the file general/system/approve_center/flow_sort/flow/delete.php. The manipulation of the argument id/sort_parent leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-	N/A	A-TON-TONG-251123/1578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			243589 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-5783**		
Affected Version(s): 2017					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Oct-2023	9.8	A vulnerability has been found in Tongda OA 2017 and classified as critical. This vulnerability affects unknown code of the file general/hr/training/record/delete.php. The manipulation of the argument RECORD_ID leads to sql injection. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. VDB-243058 is the identifier assigned to this vulnerability. NOTE: The vendor	N/A	A-TON-TONG-251123/1579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-5682**		
Vendor: torbot_project					
Product: torbot					
Affected Version(s): * Up to (excluding) 4.0.0					
N/A	18-Oct-2023	7.5	Torbot is an open source tor network intelligence tool. In affected versions the `torbot.modules.validators.validate_link function` uses the python-validators URL validation regex. This particular regular expression has an exponential complexity which allows an attacker to cause an application crash using a well-crafted argument. An attacker can use a well-crafted URL argument to exploit the vulnerability in the regular expression and cause a Denial of Service on the system. The validators file has been removed in version 4.0.0. Users	https://github.com/DedSecInside/TorBot/security/advisories/GHSA-72qw-p7hh-m3ff, https://github.com/DedSecInside/TorBot/commit/ef6e06bc7785355b1701d5524eb4550441086ac4	A-TOR-TORB-251123/1580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45813**		
Vendor: total-soft					
Product: portfolio_gallery_responsive_image_gallery					
Affected Version(s): * Up to (including) 2.0.3					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in wpdevart Gallery – Image and Video Gallery with Thumbnails plugin <= 2.0.3 versions. **CVE ID : CVE-2023-45629**	N/A	A-TOT-PORT-251123/1581
Vendor: totalpress					
Product: custom_post_types					
Affected Version(s): * Up to (including) 4.0.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in TotalPress.Org Custom post types, Custom Fields & more plugin <= 4.0.12 versions. **CVE ID : CVE-2023-32116**	N/A	A-TOT-CUST-251123/1582
Vendor: tribalsystems					
Product: zenario					
Affected Version(s): 9.4.59197					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	A Cross-Site Scripting (XSS) vulnerability in Zenario CMS v.9.4.59197 allows a local attacker to execute arbitrary code via a crafted script to the Spare aliases from Alias. **CVE ID : CVE-2023-44769**	N/A	A-TRI-ZENA-251123/1583
Vendor: triberr					
Product: triberr					
Affected Version(s): * Up to (including) 4.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Triberr plugin <= 4.1.1 versions. **CVE ID : CVE-2023-46199**	N/A	A-TRI-TRIB-251123/1584
Vendor: trteksolutions					
Product: education_portal					
Affected Version(s): * Up to (excluding) 2023-03-29					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Oct-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TRtek Software Education Portal allows SQL Injection.This issue affects Education Portal: before 3.2023.29.	N/A	A-TRT-EDUC-251123/1585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5807		
Vendor: trustedindex					
Product: widgets_for_google_reviews					
Affected Version(s): * Up to (including) 10.9					
Cross-Site Request Forgery (CSRF)	18-Oct-2023	4.3	The Widgets for Google Reviews plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 10.9. This is due to missing or incorrect nonce validation within setup_no_reg_header.php. This makes it possible for unauthenticated attackers to reset plugin settings and remove reviews via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-3254**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2980022%40wp-reviews-plugin-for-google%2Ftrunk&old=2977531%40wp-reviews-plugin-for-google%2Ftrunk&sfp_email=&sfph_mail=#file8	A-TRU-WIDG-251123/1586
Vendor: tsplus					
Product: tsplus_remote_work					
Affected Version(s): * Up to (including) 16.0.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	17-Oct-2023	9.8	TSplus Remote Work 16.0.0.0 places a cleartext password on the "var pass" line of the HTML source code for the secure single sign-on web portal. NOTE: CVE-2023-31069 is only about the TSplus Remote Access product, not the TSplus Remote Work product. **CVE ID : CVE-2023-27132**	N/A	A-TSP-TSPL-251123/1587
Incorrect Default Permissions	17-Oct-2023	9.8	TSplus Remote Work 16.0.0.0 has weak permissions for .exe, .js, and .html files under the %PROGRAMFILES(X86)%\TSplus-RemoteWork\Clients\www folder. This may enable privilege escalation if a different local user modifies a file. NOTE: CVE-2023-31067 and CVE-2023-31068 are only about the TSplus Remote Access product, not the TSplus Remote Work product. **CVE ID : CVE-2023-27133**	N/A	A-TSP-TSPL-251123/1588
Vendor: twistedmatrix					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: twisted					
Affected Version(s): * Up to (including) 22.8.0					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	25-Oct-2023	5.3	Twisted is an event-based framework for internet applications. Prior to version 23.10.0rc1, when sending multiple HTTP requests in one TCP packet, twisted.web will process the requests asynchronously without guaranteeing the response order. If one of the endpoints is controlled by an attacker, the attacker can delay the response on purpose to manipulate the response of the second request when a victim launched two requests using HTTP pipeline. Version 23.10.0rc1 contains a patch for this issue. **CVE ID : CVE-2023-46137**	https://github.com/twisted/twisted/security/advisories/GHSA-xc8x-vp79-p3wm	A-TWI-TWIS-251123/1589
Vendor: tychesoftwares					
Product: abandoned_cart_lite_for_woocommerce					
Affected Version(s): * Up to (excluding) 5.16.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Tyche Softwares Abandoned Cart Lite for WooCommerce plugin <= 5.15.2 versions. **CVE ID : CVE-2023-44986**	N/A	A-TYC-ABAN-251123/1590
Vendor: ui					
Product: unifi_network_application					
Affected Version(s): * Up to (including) 7.5.176					
N/A	25-Oct-2023	5.3	Instances of UniFi Network Application that (i) are run on a UniFi Gateway Console, and (ii) are versions 7.5.176. and earlier, implement device adoption with improper access control logic, creating a risk of access to device configuration information by a malicious actor with preexisting access to the network. Affected Products: UDM UDM-PRO UDM-SE	https://community.ui.com/releases/Security-Advisory-Bulletin-036-036/81367bc9-2a64-4435-95dc-bbe482457615	A-UI-UNIF-251123/1591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			UDR UDW Mitigation: Update UniFi Network to Version 7.5.187 or later. **CVE ID : CVE-2023-41721**		
Vendor: ultimatelysocial					
Product: social_media_share_buttons_\&_social_sharing_icons					
Affected Version(s): * Up to (excluding) 2.8.6					
Exposure of Sensitive Information to an Unauthorized Actor	20-Oct-2023	6.5	The Social Media Share Buttons & Social Sharing Icons plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 2.8.5 via the sfsi_save_export function. This can allow subscribers to export plugin settings that include social media authentication tokens and secrets as well as app passwords. **CVE ID : CVE-2023-5070**	https://www.wordfence.com/threat-intel/vulnerabilities/id/e9e43c5b-a094-44ab-a8a3-52d437f0e00d?source=cve	A-ULT-SOCI-251123/1592
Affected Version(s): * Up to (including) 2.8.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	20-Oct-2023	8.8	The Social Media Share Buttons & Social Sharing Icons plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.8.5. This is due to missing or incorrect nonce validation on several functions corresponding to AJAX actions. This makes it possible for unauthenticated attackers to invoke those actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-5602**	https://plugins.trac.wordpress.org/changeset/2975574/ultimate-social-media-icons/tags/2.8.6/libs/controllers/sfsi_buttons_controller.php?old=2956446&old_path=ultimate-social-media-icons%2Ftags%2F2.8.5%2Flibs%2Fcontrollers%2Fsfsi_buttons_controller.php	A-ULT-SOCI-251123/1593
Vendor: underdock					
Product: open_graph_metabox					
Affected Version(s): * Up to (including) 1.4.4					
Cross-Site Request Forgery (CSRF)	25-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Niels van Renselaar Open Graph Metabox plugin <= 1.4.4 versions.	N/A	A-UND-OPEN-251123/1594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46191		
Vendor: userback					
Product: userback					
Affected Version(s): * Up to (including) 1.0.13					
Cross-Site Request Forgery (CSRF)	22-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Lee Le @ Userback Userback plugin <= 1.0.13 versions. **CVE ID : CVE-2023-46089**	N/A	A-USE-USER-251123/1595
Vendor: user_location_and_ip_project					
Product: user_location_and_ip					
Affected Version(s): * Up to (including) 1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in MyTechTalky User Location and IP plugin <= 1.6 versions. **CVE ID : CVE-2023-31217**	N/A	A-USE-USER-251123/1596
Vendor: user_registration_\&_login_and_user_management_system_with_admin_panel_project					
Product: user_registration_\&_login_and_user_management_system_with_admin_panel					
Affected Version(s): 3.0					
Improper Neutralization of Special Elements used in an SQL Command	16-Oct-2023	9.8	SQL Injection vulnerability in Phpgurukul User Registration & Login and User Management System With admin panel 3.0 allows	N/A	A-USE-USER-251123/1597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			attackers to obtain sensitive information via crafted string in the admin user name field on the admin log in page. **CVE ID : CVE-2023-40852**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-2023	5.4	Cross Site Scripting (XSS) vulnerability in Phpgurukul User Registration & Login and User Management System With admin panel 3.0 allows attackers to run arbitrary code via fname, lname, email, and contact fields of the user registration page. **CVE ID : CVE-2023-40851**	N/A	A-USE-USER-251123/1598
Vendor: uvdesk					
Product: community-skeleton					
Affected Version(s): 1.1.1					
Improper Restriction of Excessive Authentication Attempts	23-Oct-2023	9.8	UVDesk Community Skeleton v1.1.1 allows unauthenticated attackers to perform brute force attacks on the login page to gain access to the application. **CVE ID : CVE-2023-37635**	N/A	A-UVD-COMM-251123/1599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: validators_project					
Product: validators					
Affected Version(s): 0.11.0					
N/A	18-Oct-2023	7.5	Torbot is an open source tor network intelligence tool. In affected versions the `torbot.modules.validators.validate_link function` uses the python-validators URL validation regex. This particular regular expression has an exponential complexity which allows an attacker to cause an application crash using a well-crafted argument. An attacker can use a well-crafted URL argument to exploit the vulnerability in the regular expression and cause a Denial of Service on the system. The validators file has been removed in version 4.0.0. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45813**	https://github.com/DedSecInside/TorBot/security/advisories/GHSA-72qw-p7hh-m3ff, https://github.com/DedSecInside/TorBot/commit/ef6e06bc7785355b1701d5524eb4550441086ac4	A-VAL-VALI-251123/1600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 0.20.0					
N/A	18-Oct-2023	7.5	Torbot is an open source tor network intelligence tool. In affected versions the `torbot.modules.validators.validate_link function` uses the python-validators URL validation regex. This particular regular expression has an exponential complexity which allows an attacker to cause an application crash using a well-crafted argument. An attacker can use a well-crafted URL argument to exploit the vulnerability in the regular expression and cause a Denial of Service on the system. The validators file has been removed in version 4.0.0. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45813**	https://github.com/DedSecInside/TorBot/security/advisories/GHSA-72qw-p7hh-m3ff, https://github.com/DedSecInside/TorBot/commit/ef6e06bc7785355b1701d5524eb4550441086ac4	A-VAL-VALI-251123/1601
Vendor: vareille					
Product: tiny_file_dialogs					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 3.15.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-Oct-2023	9.8	tinyfiledialogs (aka tiny file dialogs) before 3.15.0 allows shell metacharacters (such as a backquote or a dollar sign) in titles, messages, and other input data. NOTE: this issue exists because of an incomplete fix for CVE-2020-36767, which only considered single and double quote characters. **CVE ID : CVE-2023-47104**	https://sourceforge.net/p/tinyfiledialogs/code/ci/ac9f9f6d8cdf45ca8d9b4cf1f201ee472301e114/	A-VAR-TINY-251123/1602
Vendor: varktech					
Product: minimum_purchase_for_woocommerce					
Affected Version(s): * Up to (including) 2.0.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Vark Minimum Purchase for WooCommerce plugin <= 2.0.0.1 versions. **CVE ID : CVE-2023-30492**	N/A	A-VAR-MINI-251123/1603
Vendor: vektor-inc					
Product: vk_filter_search					
Affected Version(s): * Up to (including) 2.3.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Oct-2023	5.4	The VK Filter Search plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'vk_filter_search' shortcode in all versions up to, and including, 2.3.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5705**	https://plugins.trac.wordpress.org/changeset/2983339/vk-filter-search#file1	A-VEK-VK_F-251123/1604
Vendor: vercel					
Product: next.js					
Affected Version(s): * Up to (excluding) 13.4.20					
N/A	22-Oct-2023	7.5	Next.js before 13.4.20-canary.13 lacks a cache-control header and thus empty prefetch responses may sometimes be cached by a CDN,	https://github.com/vercel/next.js/pull/54732	A-VER-NEXT-251123/1605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causing a denial of service to all users requesting the same URL via that CDN. **CVE ID : CVE-2023-46298**		
Affected Version(s): 13.4.20					
N/A	22-Oct-2023	7.5	Next.js before 13.4.20-canary.13 lacks a cache-control header and thus empty prefetch responses may sometimes be cached by a CDN, causing a denial of service to all users requesting the same URL via that CDN. **CVE ID : CVE-2023-46298**	https://github.com/vercel/next.js/pull/54732	A-VER-NEXT-251123/1606
Vendor: very_simple_google_maps_project					
Product: very_simple_google_maps					
Affected Version(s): * Up to (including) 2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	The Very Simple Google Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'vsgmap' shortcode in all versions up to, and including, 2.9 due to insufficient input sanitization and output escaping on user supplied attributes.	https://plugins.trac.wordpress.org/changeset/2982539/very-simple-google-maps#file1	A-VER-VERY-251123/1607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5744**		
Vendor: VIM					
Product: vim					
Affected Version(s): * Up to (excluding) 9.0.2068					
Integer Overflow or Wraparound	27-Oct-2023	5.5	Vim is an improved version of the good old UNIX editor Vi. Heap-use-after-free in memory allocated in the function `ga_grow_inner` in in the file `src/alloc.c` at line 748, which is freed in the file `src/ex_docmd.c` in the function `do_cmdline` at line 1010 and then used again in `src/cmdhist.c` at line 759. When using the `:history` command, it's possible that the provided argument overflows the	https://github.com/vim/vim/commit/9198c1f2b1ddecde22af918541e0de2a32f0f45a	A-VIM-VIM-251123/1608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accepted value. Causing an Integer Overflow and potentially later an use-after-free. This vulnerability has been patched in version 9.0.2068. **CVE ID : CVE-2023-46246**		
Vendor: virtuellwerk					
Product: canvasio3d_light					
Affected Version(s): * Up to (including) 2.4.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Thomas Scholl canvasio3D Light plugin <= 2.4.6 versions. **CVE ID : CVE-2023-45062**	N/A	A-VIR-CANV-251123/1609
Vendor: Vmware					
Product: aria_operations_for_logs					
Affected Version(s): 5.0					
Incorrect Authorization	20-Oct-2023	9.8	VMware Aria Operations for Logs contains an authentication bypass vulnerability. An unauthenticated, malicious actor can inject files into the operating system of an impacted appliance which can result in	https://www.vmware.com/security/advisories/VMSA-2023-0021.html	A-VMW-ARIA-251123/1610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution. **CVE ID : CVE-2023-34051**		
Deserialization of Untrusted Data	20-Oct-2023	7.8	VMware Aria Operations for Logs contains a deserialization vulnerability. A malicious actor with non-administrative access to the local system can trigger the deserialization of data which could result in authentication bypass. **CVE ID : CVE-2023-34052**	https://www.vmware.com/security/advisories/VMSA-2023-0021.html	A-VMW-ARIA-251123/1611
Affected Version(s): 4.0					
Incorrect Authorization	20-Oct-2023	9.8	VMware Aria Operations for Logs contains an authentication bypass vulnerability. An unauthenticated, malicious actor can inject files into the operating system of an impacted appliance which can result in remote code execution.	https://www.vmware.com/security/advisories/VMSA-2023-0021.html	A-VMW-ARIA-251123/1612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34051		
Deserialization of Untrusted Data	20-Oct-2023	7.8	VMware Aria Operations for Logs contains a deserialization vulnerability. A malicious actor with non-administrative access to the local system can trigger the deserialization of data which could result in authentication bypass. **CVE ID : CVE-2023-34052**	https://www.vmware.com/security/advisories/VMSA-2023-0021.html	A-VMW-ARIA-251123/1613
Affected Version(s): 8.10					
Incorrect Authorization	20-Oct-2023	9.8	VMware Aria Operations for Logs contains an authentication bypass vulnerability. An unauthenticated, malicious actor can inject files into the operating system of an impacted appliance which can result in remote code execution. **CVE ID : CVE-2023-34051**	https://www.vmware.com/security/advisories/VMSA-2023-0021.html	A-VMW-ARIA-251123/1614
Affected Version(s): 8.10.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	20-Oct-2023	9.8	VMware Aria Operations for Logs contains an authentication bypass vulnerability. An unauthenticated, malicious actor can inject files into the operating system of an impacted appliance which can result in remote code execution. **CVE ID : CVE-2023-34051**	https://www.vmware.com/security/advisories/VMSA-2023-0021.html	A-VMW-ARIA-251123/1615
Deserialization of Untrusted Data	20-Oct-2023	7.8	VMware Aria Operations for Logs contains a deserialization vulnerability. A malicious actor with non-administrative access to the local system can trigger the deserialization of data which could result in authentication bypass. **CVE ID : CVE-2023-34052**	https://www.vmware.com/security/advisories/VMSA-2023-0021.html	A-VMW-ARIA-251123/1616
Affected Version(s): 8.12					
Incorrect Authorization	20-Oct-2023	9.8	VMware Aria Operations for Logs contains an authentication bypass	https://www.vmware.com/security/advisories	A-VMW-ARIA-251123/1617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. An unauthenticated, malicious actor can inject files into the operating system of an impacted appliance which can result in remote code execution. **CVE ID : CVE-2023-34051**	/VMSA-2023-0021.html	
Deserialization of Untrusted Data	20-Oct-2023	7.8	VMware Aria Operations for Logs contains a deserialization vulnerability. A malicious actor with non-administrative access to the local system can trigger the deserialization of data which could result in authentication bypass. **CVE ID : CVE-2023-34052**	https://www.vmware.com/security/advisories/VMSA-2023-0021.html	A-VMW-ARIA-251123/1618
Affected Version(s): 8.6					
Incorrect Authorization	20-Oct-2023	9.8	VMware Aria Operations for Logs contains an authentication bypass vulnerability. An unauthenticated, malicious actor can inject files into the operating system	https://www.vmware.com/security/advisories/VMSA-2023-0021.html	A-VMW-ARIA-251123/1619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of an impacted appliance which can result in remote code execution. **CVE ID : CVE-2023-34051**		
Affected Version(s): 8.8					
Incorrect Authorization	20-Oct-2023	9.8	VMware Aria Operations for Logs contains an authentication bypass vulnerability. An unauthenticated, malicious actor can inject files into the operating system of an impacted appliance which can result in remote code execution. **CVE ID : CVE-2023-34051**	https://www.vmware.com/security/advisories/VMSA-2023-0021.html	A-VMW-ARIA-251123/1620
Product: fusion					
Affected Version(s): From (including) 13.0.0 Up to (excluding) 13.5					
N/A	20-Oct-2023	7.8	VMware Fusion(13.x prior to 13.5) contains a local privilege escalation vulnerability that occurs during installation for the first time (the user needs to drag or copy the	https://www.vmware.com/security/advisories/VMSA-2023-0022.html	A-VMW-FUSI-251123/1621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system where Fusion is installed or being installed for the first time. **CVE ID : CVE-2023-34045**		
Time-of-check Time-of-use (TOCTOU) Race Condition	20-Oct-2023	7	VMware Fusion(13.x prior to 13.5) contains a TOCTOU (Time-of-check Time-of-use) vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may	https://www.vmware.com/security/advisories/VMSA-2023-0022.html	A-VMW-FUSI-251123/1622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability to escalate privileges to root on the system where Fusion is installed or being installed for the first time. **CVE ID : CVE-2023-34046**		
Out-of-bounds Read	20-Oct-2023	6	VMware Workstation(17.x prior to 17.5) and Fusion(13.x prior to 13.5) contain an out-of-bounds read vulnerability that exists in the functionality for sharing host Bluetooth devices with the virtual machine. A malicious actor with local administrative privileges on a virtual machine may be able to read privileged information contained in hypervisor memory from a virtual machine. **CVE ID : CVE-2023-34044**	https://www.vmware.com/security/advisories/VMSA-2023-0022.html	A-VMW-FUSI-251123/1623
Product: open_vm_tools					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 11.0.0 Up to (including) 12.3.0					
Improper Verification of Cryptographic Signature	27-Oct-2023	7.5	VMware Tools contains a SAML token signature bypass vulnerability. A malicious actor that has been granted Guest Operation Privileges https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-6A952214-0E5E-4CCF-9D2A-90948FF643EC.html in a target virtual machine may be able to elevate their privileges if that target virtual machine has been assigned a more privileged Guest Alias https://vdc-download.vmware.com/vmwb-repository/dcr-public/d1902b0e-d479-46bf-8ac9-cee0e31e8ec0/07ce8dbd-db48-4261-9b8f-c6d3ad8ba472/vim.vm.guest.AliasManager.html . **CVE ID : CVE-2023-34058**	https://www.vmware.com/security/advisories/VMSA-2023-0024.html, http://www.openwall.com/lists/oss-security/2023/10/27/1	A-VMW-OPEN-251123/1624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Oct-2023	7	open-vm-tools contains a file descriptor hijack vulnerability in the vmware-user-suid-wrapper. A malicious actor with non-root privileges may be able to hijack the /dev/uinput file descriptor allowing them to simulate user inputs. **CVE ID : CVE-2023-34059**	http://www.openwall.com/lists/oss-security/2023/10/27/2	A-VMW-OPEN-251123/1625
Product: rabbitmq					
Affected Version(s): * Up to (excluding) 3.11.24					
Uncontrolled Resource Consumption	25-Oct-2023	4.9	RabbitMQ is a multi-protocol messaging and streaming broker. HTTP API did not enforce an HTTP request body limit, making it vulnerable for denial of service (DoS) attacks with very large messages. An authenticated user with sufficient credentials can publish a very large messages over the HTTP API and cause target node to be terminated by an "out-of-memory killer"-like	https://github.com/rabbitmq/rabbitmq-server/security/advisories/GHSA-w6cq-9cf4-gqpg	A-VMW-RABB-251123/1626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mechanism. This vulnerability has been patched in versions 3.11.24 and 3.12.7. **CVE ID : CVE-2023-46118**		
Affected Version(s): From (including) 3.12.0 Up to (excluding) 3.12.7					
Uncontrolled Resource Consumption	25-Oct-2023	4.9	RabbitMQ is a multi-protocol messaging and streaming broker. HTTP API did not enforce an HTTP request body limit, making it vulnerable for denial of service (DoS) attacks with very large messages. An authenticated user with sufficient credentials can publish a very large messages over the HTTP API and cause target node to be terminated by an "out-of-memory killer"-like mechanism. This vulnerability has been patched in versions 3.11.24 and 3.12.7. **CVE ID : CVE-2023-46118**	https://github.com/rabbitmq/rabbitmq-server/security/advisories/GHSA-w6cq-9cf4-gqpg	A-VMW-RABB-251123/1627
Product: rabbitmq_java_client					
Affected Version(s): * Up to (excluding) 5.18.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	25-Oct-2023	7.5	The RabbitMQ Java client library allows Java and JVM-based applications to connect to and interact with RabbitMQ nodes. `maxBodyLebgth` was not used when receiving Message objects. Attackers could send a very large Message causing a memory overflow and triggering an OOM Error. Users of RabbitMQ may suffer from DoS attacks from RabbitMQ Java client which will ultimately exhaust the memory of the consumer. This vulnerability was patched in version 5.18.0. **CVE ID : CVE-2023-46120**	https://github.com/rabbitmq/rabbitmq-java-client/issues/1062, https://github.com/rabbitmq/rabbitmq-java-client/security/advisories/GHSA-mm8h-8587-p46h, https://github.com/rabbitmq/rabbitmq-java-client/commit/714aae602dcae6cb4b53cadf009323ebac313cc8	A-VMW-RABB-251123/1628
Product: spring_advanced_message_queuing_protocol					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 2.4.16					
Deserialization of Untrusted Data	19-Oct-2023	4.3	In spring AMQP versions 1.0.0 to 2.4.16 and 3.0.0 to 3.0.9 , allowed list patterns for deserializable class names were added to Spring AMQP,	https://spring.io/security/cve-2023-34050	A-VMW-SPRI-251123/1629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowing users to lock down deserialization of data in messages from untrusted sources; however by default, when no allowed list was provided, all classes could be deserialized. Specifically, an application is vulnerable if * the SimpleMessageConverter or SerializerMessageConverter is used * the user does not configure allowed list patterns * untrusted message originators gain permissions to write messages to the RabbitMQ broker to send malicious content **CVE ID : CVE-2023-34050**		
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.9					
Deserialization of Untrusted Data	19-Oct-2023	4.3	In spring AMQP versions 1.0.0 to 2.4.16 and 3.0.0 to 3.0.9 , allowed list	https://spring.io/security/cve-2023-34050	A-VMW-SPRI-251123/1630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patterns for deserializable class names were added to Spring AMQP, allowing users to lock down deserialization of data in messages from untrusted sources; however by default, when no allowed list was provided, all classes could be deserialized. Specifically, an application is vulnerable if * the SimpleMessageConverter or SerializerMessageConverter is used * the user does not configure allowed list patterns * untrusted message originators gain permissions to write messages to the RabbitMQ broker to send malicious content **CVE ID : CVE-2023-34050**		
Product: spring_boot					
Affected Version(s): * Up to (excluding) 1.37.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Oct-2023	9.8	An issue in Dromara SaToken version 1.36.0 and before allows a remote attacker to escalate privileges via a crafted payload to the URL. **CVE ID : CVE-2023-44794**	https://github.com/dromara/Sa-Token/issues/515	A-VMW-SPRI-251123/1631
Product: spring_framework					
Affected Version(s): * Up to (excluding) 1.37.0					
N/A	25-Oct-2023	9.8	An issue in Dromara SaToken version 1.36.0 and before allows a remote attacker to escalate privileges via a crafted payload to the URL. **CVE ID : CVE-2023-44794**	https://github.com/dromara/Sa-Token/issues/515	A-VMW-SPRI-251123/1632
Product: tools					
Affected Version(s): From (including) 10.3.0 Up to (excluding) 12.1.1					
Improper Privilege Management	27-Oct-2023	7.8	VMware Tools contains a local privilege escalation vulnerability. A malicious actor with local user access to a guest virtual machine may elevate privileges within the virtual machine. **CVE ID : CVE-2023-34057**	https://www.vmware.com/security/advisories/VMSA-2023-0024.html	A-VMW-TOOL-251123/1633
Affected Version(s): From (including) 10.3.0 Up to (excluding) 12.3.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Verification of Cryptographic Signature	27-Oct-2023	7.5	VMware Tools contains a SAML token signature bypass vulnerability. A malicious actor that has been granted Guest Operation Privileges https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-6A952214-0E5E-4CCF-9D2A-90948FF643EC.html in a target virtual machine may be able to elevate their privileges if that target virtual machine has been assigned a more privileged Guest Alias https://vdc-download.vmware.com/vmwb-repository/dcr-public/d1902b0e-d479-46bf-8ac9-cee0e31e8ec0/07ce8dbd-db48-4261-9b8f-c6d3ad8ba472/vim.vm.guest.AliasManager.html . **CVE ID : CVE-2023-34058**	https://www.vmware.com/security/advisories/VMSA-2023-0024.html, http://www.openwall.com/lists/oss-security/2023/10/27/1	A-VMW-TOOL-251123/1634
Product: vcenter_server					
Affected Version(s): 7.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	25-Oct-2023	9.8	vCenter Server contains an out-of-bounds write vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger an out-of-bounds write potentially leading to remote code execution. **CVE ID : CVE-2023-34048**	https://www.vmware.com/security/advisories/VMSA-2023-0023.html	A-VMW-VCEN-251123/1635
N/A	25-Oct-2023	4.3	vCenter Server contains a partial information disclosure vulnerability. A malicious actor with non-administrative privileges to vCenter Server may leverage this issue to access unauthorized data. **CVE ID : CVE-2023-34056**	https://www.vmware.com/security/advisories/VMSA-2023-0023.html	A-VMW-VCEN-251123/1636
Affected Version(s): 8.0					
Out-of-bounds Write	25-Oct-2023	9.8	vCenter Server contains an out-of-bounds write vulnerability in the implementation of the DCERPC protocol. A malicious actor with network	https://www.vmware.com/security/advisories/VMSA-2023-0023.html	A-VMW-VCEN-251123/1637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to vCenter Server may trigger an out-of-bounds write potentially leading to remote code execution. **CVE ID : CVE-2023-34048**		
N/A	25-Oct-2023	4.3	vCenter Server contains a partial information disclosure vulnerability. A malicious actor with non-administrative privileges to vCenter Server may leverage this issue to access unauthorized data. **CVE ID : CVE-2023-34056**	https://www.vmware.com/security/advisories/VMSA-2023-0023.html	A-VMW-VCEN-251123/1638
Affected Version(s): From (including) 4.0 Up to (including) 5.5					
Out-of-bounds Write	25-Oct-2023	9.8	vCenter Server contains an out-of-bounds write vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger an out-of-bounds write potentially leading to remote code execution. **CVE ID : CVE-2023-34048**	https://www.vmware.com/security/advisories/VMSA-2023-0023.html	A-VMW-VCEN-251123/1639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Oct-2023	4.3	vCenter Server contains a partial information disclosure vulnerability. A malicious actor with non-administrative privileges to vCenter Server may leverage this issue to access unauthorized data. **CVE ID : CVE-2023-34056**	https://www.vmware.com/security/advisories/VMSA-2023-0023.html	A-VMW-VCEN-251123/1640
Product: workstation					
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.5					
Out-of-bounds Read	20-Oct-2023	6	VMware Workstation(17.x prior to 17.5) and Fusion(13.x prior to 13.5) contain an out-of-bounds read vulnerability that exists in the functionality for sharing host Bluetooth devices with the virtual machine. A malicious actor with local administrative privileges on a virtual machine may be able to read privileged information contained in	https://www.vmware.com/security/advisories/VMSA-2023-0022.html	A-VMW-WORK-251123/1641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hypervisor memory from a virtual machine. **CVE ID : CVE-2023-34044**		
Vendor: vnote_project					
Product: vnote					
Affected Version(s): * Up to (including) 3.17.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	6.1	A vulnerability has been found in vnotex vnote up to 3.17.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Markdown File Handler. The manipulation with the input <xss onclick="alert(1)" style=display:block >Click here</xss> 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-243139. NOTE: The vendor was contacted early about this disclosure but did	N/A	A-VNO-VNOT-251123/1642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not respond in any way. **CVE ID : CVE-2023-5701**		
Vendor: vuejs					
Product: devtools					
Affected Version(s): 6.5.0					
Origin Validation Error	23-Oct-2023	4.3	The Vue.js Devtools extension was found to leak screenshot data back to a malicious web page via the standard `postMessage()` API. By creating a malicious web page with an iFrame targeting a sensitive resource (i.e. a locally accessible file or sensitive website), and registering a listener on the web page, the extension sent messages back to the listener, containing the base64 encoded screenshot data of the sensitive resource. **CVE ID : CVE-2023-5718**	https://gist.github.com/CalumHutton/bdb97077a66021ed455f87823cd7c7cb	A-VUE-DEVT-251123/1643
Vendor: wagtail					
Product: wagtail					
Affected Version(s): * Up to (excluding) 4.1.9					
Insertion of Sensitive Informatio	19-Oct-2023	2.7	Wagtail is an open source content management	https://github.com/wagtail/wagtail/security/a	A-WAG-WAGT-251123/1644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n into Log File			system built on Django. A user with a limited-permission editor account for the Wagtail admin can make a direct URL request to the admin view that handles bulk actions on user accounts. While authentication rules prevent the user from making any changes, the error message discloses the display names of user accounts, and by modifying URL parameters, the user can retrieve the display name for any user. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. Patched versions have been released as Wagtail 4.1.8 (LTS), 5.0.5 and 5.1.3. The fix is also included in Release Candidate 1 of the forthcoming Wagtail 5.2 release. Users are advised to upgrade. There are no known	dvisories/GHSA-fc75-58r8-rm3h, https://github.com/wagtail/wagtail/commit/bc96aed6ac53f998b2f4c4bf97e2d4f5fe337e5b	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds for this vulnerability. **CVE ID : CVE-2023-45809**		
Affected Version(s): From (including) 4.2 Up to (excluding) 5.0.5					
Insertion of Sensitive Information into Log File	19-Oct-2023	2.7	Wagtail is an open source content management system built on Django. A user with a limited-permission editor account for the Wagtail admin can make a direct URL request to the admin view that handles bulk actions on user accounts. While authentication rules prevent the user from making any changes, the error message discloses the display names of user accounts, and by modifying URL parameters, the user can retrieve the display name for any user. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. Patched versions have been released as Wagtail 4.1.8 (LTS), 5.0.5 and	https://github.com/wagtail/wagtail/security/advisories/GHSA-fc75-58r8-rm3h, https://github.com/wagtail/wagtail/commit/bc96aed6ac53f998b2f4c4bf97e2d4f5fe337e5b	A-WAG-WAGT-251123/1645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5.1.3. The fix is also included in Release Candidate 1 of the forthcoming Wagtail 5.2 release. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45809**		
Affected Version(s): From (including) 5.1 Up to (excluding) 5.1.3					
Insertion of Sensitive Information into Log File	19-Oct-2023	2.7	Wagtail is an open source content management system built on Django. A user with a limited-permission editor account for the Wagtail admin can make a direct URL request to the admin view that handles bulk actions on user accounts. While authentication rules prevent the user from making any changes, the error message discloses the display names of user accounts, and by modifying URL parameters, the user can retrieve the display name for any user. The vulnerability is not exploitable by an	https://github.com/wagtail/wagtail/security/advisories/GHSA-fc75-58r8-rm3h, https://github.com/wagtail/wagtail/commit/bc96aed6ac53f998b2f4c4bf97e2d4f5fe337e5b	A-WAG-WAGT-251123/1646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ordinary site visitor without access to the Wagtail admin. Patched versions have been released as Wagtail 4.1.8 (LTS), 5.0.5 and 5.1.3. The fix is also included in Release Candidate 1 of the forthcoming Wagtail 5.2 release. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45809**		
Vendor: wallix					
Product: bastion					
Affected Version(s): * Up to (excluding) 9.0.9					
N/A	23-Oct-2023	7.5	WALLIX Bastion 9.x before 9.0.9 and 10.x before 10.0.5 allows unauthenticated access to sensitive information by bypassing access control on a network access administration web interface. **CVE ID : CVE-2023-46319**	https://www.wallix.com/support/alerts/	A-WAL-BAST-251123/1647
Affected Version(s): From (including) 10.0 Up to (excluding) 10.0.5					
N/A	23-Oct-2023	7.5	WALLIX Bastion 9.x before 9.0.9 and 10.x before 10.0.5	https://www.wallix.com/support/alerts/	A-WAL-BAST-251123/1648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated access to sensitive information by bypassing access control on a network access administration web interface. **CVE ID : CVE-2023-46319**		
Vendor: wandlesoftware					
Product: smart_app_banner					
Affected Version(s): * Up to (including) 1.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Stephen Darlington, Wandle Software Limited Smart App Banner plugin <= 1.1.3 versions. **CVE ID : CVE-2023-46200**	N/A	A-WAN-SMAR-251123/1649
Vendor: Wbce					
Product: wbce_cms					
Affected Version(s): * Up to (including) 1.6.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-2023	5.4	Cross Site Scripting (XSS) vulnerability in WBCE CMS v.1.6.1 and before allows a remote attacker to escalate privileges via a crafted script to the website_footer parameter in the	N/A	A-WBC-WBCE-251123/1650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin/settings/save.php component. **CVE ID : CVE-2023-46054**		
Vendor: weavertheme					
Product: weaver_xtreme_theme_support					
Affected Version(s): * Up to (excluding) 6.3.1					
Deserialization of Untrusted Data	16-Oct-2023	7.2	The Weaver Xtreme Theme Support WordPress plugin before 6.3.1 unserialises the content of an imported file, which could lead to PHP object injections issues when a high privilege user import a malicious file and a suitable gadget chain is present on the blog. **CVE ID : CVE-2023-4971**	N/A	A-WEA-WEAV-251123/1651
Vendor: web-audimex					
Product: audimex					
Affected Version(s): 15.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	Audimex 15.0.0 is vulnerable to Cross Site Scripting (XSS) in /audimex/cgi-bin/wal.fcgi via company parameter search filters. **CVE ID : CVE-2023-46396**	N/A	A-WEB-AUDI-251123/1652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Web-dorado					
Product: spidervplayer					
Affected Version(s): * Up to (including) 1.5.22					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WebDorado SpiderVPlayer plugin <= 1.5.22 versions. **CVE ID : CVE-2023-45632**	N/A	A-WEB-SPID-251123/1653
Product: wdsocialwidgets					
Affected Version(s): * Up to (including) 1.0.15					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WebDorado WDSocialWidgets plugin <= 1.0.15 versions. **CVE ID : CVE-2023-46090**	N/A	A-WEB-WDSO-251123/1654
Vendor: Web2py					
Product: web2py					
Affected Version(s): * Up to (including) 2.24.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Oct-2023	9.8	An OS command injection vulnerability exists in web2py 2.24.1 and earlier. When the product is configured to use notifySendHandler for logging (not the default configuration), a crafted web request may execute an	https://github.com/web2py/web2py/commit/936e2260b0c34c44e2f3674a893e96d2a7fad0a3	A-WEB-WEB2-251123/1655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary OS command on the web server using the product. **CVE ID : CVE-2023-45158**		
Vendor: webassembly					
Product: webassembly_binary_toolkit					
Affected Version(s): 1.0.33					
Out-of-bounds Read	23-Oct-2023	5.5	WebAssembly wabt 1.0.33 has an Out-of-Bound Memory Read in in DataSegment::IsValidRange(), which lead to segmentation fault. **CVE ID : CVE-2023-46331**	https://github.com/WebAssembly/wabt/issues/2310	A-WEB-WEBA-251123/1656
Out-of-bounds Write	23-Oct-2023	5.5	WebAssembly wabt 1.0.33 contains an Out-of-Bound Memory Write in DataSegment::Drop(), which lead to segmentation fault. **CVE ID : CVE-2023-46332**	https://github.com/WebAssembly/wabt/issues/2311	A-WEB-WEBA-251123/1657
Vendor: webauthn4j					
Product: spring_security					
Affected Version(s): * Up to (excluding) 0.9.1					
Improper Authentication	16-Oct-2023	5.3	WebAuthn4J Spring Security provides Web Authentication specification support for Spring applications. Affected versions	https://github.com/webauthn4j/webauthn4j-spring-security/commit/129700d74d83f9b9a82bf88ebc63707e3cb0a	A-WEB-SPRI-251123/1658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are subject to improper signature counter value handling. A flaw was found in webauthn4j-spring-security-core. When an authneticator returns an incremented signature counter value during authentication, webauthn4j-spring-security-core does not properly persist the value, which means cloned authenticator detection does not work. An attacker who cloned valid authenticator in some way can use the cloned authenticator without being detected. This issue has been addressed in version `0.9.1.RELEASE`. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-45669**	725, https://github.com/webauthn4j/webauthn4j-spring-security/security/advisories/GHSA-v9hx-v6vf-g36j	
Vendor: webcource					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wc_captcha					
Affected Version(s): * Up to (including) 1.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WebCource WC Captcha plugin <= 1.4 versions. **CVE ID : CVE-2023-46210**	N/A	A-WEB-WC_C-251123/1659
Vendor: Webkul					
Product: uvdesk					
Affected Version(s): 1.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-2023	5.4	A stored cross-site scripting (XSS) vulnerability in UVDesk Community Skeleton v1.1.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Message field when creating a ticket. **CVE ID : CVE-2023-37636**	N/A	A-WEB-UVDE-251123/1660
Vendor: webnus					
Product: modern_events_calendar_lite					
Affected Version(s): * Up to (excluding) 7.1.0					
Improper Neutralization of Input During Web Page Generation	20-Oct-2023	4.8	The Modern Events Calendar lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Google API key and	https://webnus.net/modern-events-calendar/change-log/	A-WEB-MODE-251123/1661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Calendar ID in versions up to, but not including, 7.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-4021**		
Vendor: webshopworks					
Product: creativepopup					
Affected Version(s): * Up to (excluding) 1.6.10					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Oct-2023	9.8	In the module "Creative Popup" (creativepopup) up to version 1.6.9 from WebshopWorks for PrestaShop, a guest can perform SQL injection via `cp_download_popup().`	N/A	A-WEB-CREA-251123/1662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45381		
Vendor: wenwen-ai					
Product: wenwenai_cms					
Affected Version(s): 1.0					
Incorrect Default Permissions	25-Oct-2023	8	Insecure Permissions vulnerability in WenwenaiCMS v.1.0 allows a remote attacker to escalate privileges. **CVE ID : CVE-2023-45990**	N/A	A-WEN-WENW-251123/1663
Vendor: wiloke					
Product: your_journey					
Affected Version(s): * Up to (including) 1.9.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	6.1	The Your Journey theme for WordPress is vulnerable to Reflected Cross-Site Scripting via prototype pollution in versions up to, and including, 1.9.8 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	N/A	A-WIL-YOUR-251123/1664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action such as clicking on a link. **CVE ID : CVE-2023-3933**		
Vendor: wipotec					
Product: comscale					
Affected Version(s): 4.3.29.21344					
Exposure of Resource to Wrong Sphere	18-Oct-2023	9.8	An issue in WIPOTEC GmbH ComScale v4.3.29.21344 and v4.4.12.723 allows unauthenticated attackers to login as any user without a password. **CVE ID : CVE-2023-45911**	N/A	A-WIP-COMS-251123/1665
Exposure of Sensitive Information to an Unauthorized Actor	18-Oct-2023	7.5	WIPOTEC GmbH ComScale v4.3.29.21344 and v4.4.12.723 fails to validate user sessions, allowing unauthenticated attackers to read files from the underlying operating system and obtain directory listings. **CVE ID : CVE-2023-45912**	N/A	A-WIP-COMS-251123/1666
Affected Version(s): 4.4.12.723					
Exposure of Resource to Wrong Sphere	18-Oct-2023	9.8	An issue in WIPOTEC GmbH ComScale v4.3.29.21344 and v4.4.12.723 allows unauthenticated attackers to login	N/A	A-WIP-COMS-251123/1667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as any user without a password. **CVE ID : CVE-2023-45911**		
Exposure of Sensitive Information to an Unauthorized Actor	18-Oct-2023	7.5	WIPOTEC GmbH ComScale v4.3.29.21344 and v4.4.12.723 fails to validate user sessions, allowing unauthenticated attackers to read files from the underlying operating system and obtain directory listings. **CVE ID : CVE-2023-45912**	N/A	A-WIP-COMS-251123/1668
Vendor: Wokamoto					
Product: simple_tweet					
Affected Version(s): * Up to (including) 1.4.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Wokamoto Simple Tweet plugin <= 1.4.0.2 versions. **CVE ID : CVE-2023-45767**	N/A	A-WOK-SIMP-251123/1669
Vendor: Wordpress					
Product: wordpress					
Affected Version(s): From (including) 4.7 Up to (excluding) 4.7.27					
N/A	16-Oct-2023	5.3	The Popup Builder WordPress plugin through 4.1.15 does not sanitise and escape some of its settings, which	N/A	A-WOR-WORD-251123/1670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-5561**		
Affected Version(s): From (including) 4.8 Up to (excluding) 4.8.23					
N/A	16-Oct-2023	5.3	The Popup Builder WordPress plugin through 4.1.15 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-2023-5561**	N/A	A-WOR-WORD-251123/1671
Affected Version(s): From (including) 4.9 Up to (excluding) 4.9.24					
N/A	16-Oct-2023	5.3	The Popup Builder WordPress plugin through 4.1.15 does not sanitise and escape some of its settings, which could allow high privilege users	N/A	A-WOR-WORD-251123/1672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-5561**		
Affected Version(s): From (including) 5.0 Up to (excluding) 5.0.20					
N/A	16-Oct-2023	5.3	The Popup Builder WordPress plugin through 4.1.15 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-2023-5561**	N/A	A-WOR-WORD-251123/1673
Affected Version(s): From (including) 5.1 Up to (excluding) 5.1.17					
N/A	16-Oct-2023	5.3	The Popup Builder WordPress plugin through 4.1.15 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored	N/A	A-WOR-WORD-251123/1674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID : CVE-2023-5561**		
Affected Version(s): From (including) 5.2 Up to (excluding) 5.2.19					
N/A	16-Oct-2023	5.3	The Popup Builder WordPress plugin through 4.1.15 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-2023-5561**	N/A	A-WOR-WORD-251123/1675
Affected Version(s): From (including) 5.3 Up to (excluding) 5.3.16					
N/A	16-Oct-2023	5.3	The Popup Builder WordPress plugin through 4.1.15 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	N/A	A-WOR-WORD-251123/1676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID : CVE-2023-5561**		
Affected Version(s): From (including) 5.4 Up to (excluding) 5.4.14					
N/A	16-Oct-2023	5.3	The Popup Builder WordPress plugin through 4.1.15 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-2023-5561**	N/A	A-WOR-WORD-251123/1677
Affected Version(s): From (including) 5.5 Up to (excluding) 5.5.13					
N/A	16-Oct-2023	5.3	The Popup Builder WordPress plugin through 4.1.15 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	N/A	A-WOR-WORD-251123/1678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disallowed (for example in multisite setup). **CVE ID : CVE-2023-5561**		
Affected Version(s): From (including) 5.6 Up to (excluding) 5.6.12					
N/A	16-Oct-2023	5.3	The Popup Builder WordPress plugin through 4.1.15 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-2023-5561**	N/A	A-WOR-WORD-251123/1679
Affected Version(s): From (including) 5.7 Up to (excluding) 5.7.10					
N/A	16-Oct-2023	5.3	The Popup Builder WordPress plugin through 4.1.15 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	N/A	A-WOR-WORD-251123/1680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			example in multisite setup). **CVE ID : CVE-2023-5561**		
Affected Version(s): From (including) 5.8 Up to (excluding) 5.8.8					
N/A	16-Oct-2023	5.3	The Popup Builder WordPress plugin through 4.1.15 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-2023-5561**	N/A	A-WOR-WORD-251123/1681
Affected Version(s): From (including) 5.9 Up to (excluding) 5.9.8					
N/A	16-Oct-2023	5.3	The Popup Builder WordPress plugin through 4.1.15 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-WOR-WORD-251123/1682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5561		
Affected Version(s): From (including) 6.0 Up to (excluding) 6.0.6					
N/A	16-Oct-2023	5.3	The Popup Builder WordPress plugin through 4.1.15 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-2023-5561**	N/A	A-WOR-WORD-251123/1683
Affected Version(s): From (including) 6.1 Up to (excluding) 6.1.4					
N/A	16-Oct-2023	5.3	The Popup Builder WordPress plugin through 4.1.15 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-2023-5561**	N/A	A-WOR-WORD-251123/1684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 6.2 Up to (excluding) 6.2.3					
N/A	16-Oct-2023	5.3	The Popup Builder WordPress plugin through 4.1.15 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-2023-5561**	N/A	A-WOR-WORD-251123/1685
Affected Version(s): From (including) 6.3 Up to (excluding) 6.3.2					
N/A	16-Oct-2023	5.3	The Popup Builder WordPress plugin through 4.1.15 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-2023-5561**	N/A	A-WOR-WORD-251123/1686
Vendor: wordpress_popular_posts_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wordpress_popular_posts					
Affected Version(s): * Up to (excluding) 6.3.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Hector Cabrera WordPress Popular Posts plugin <= 6.3.2 versions. **CVE ID : CVE-2023-45607**	N/A	A-WOR-WORD-251123/1687
Vendor: wp-pizza					
Product: wppizza					
Affected Version(s): * Up to (excluding) 3.18.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ollybach WPPizza – A Restaurant Plugin plugin <= 3.18.2 versions. **CVE ID : CVE-2023-46622**	N/A	A-WP--WPPI-251123/1688
Vendor: wp-slimstat					
Product: slimstat_analytics					
Affected Version(s): * Up to (excluding) 5.0.10					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Oct-2023	6.5	The Slimstat Analytics plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 5.0.9 due to insufficient escaping on the user supplied	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2959452%40wp-slimstat&new=2959452%40wp-slimstat&sfp_e	A-WP--SLIM-251123/1689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with contributor-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-4598**	mail=&sfph_mail=	
Vendor: wp3sixty					
Product: woo_custom_emails					
Affected Version(s): * Up to (including) 2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in wp3sixty Woo Custom Emails plugin <= 2.2 versions. **CVE ID : CVE-2023-45004**	N/A	A-WP3-WOO_-251123/1690
Vendor: wpbookingcalendar					
Product: booking_calendar					
Affected Version(s): * Up to (excluding) 9.7.3.1					
N/A	16-Oct-2023	6.1	The Booking Calendar WordPress plugin before 9.7.3.1 does not sanitize and	N/A	A-WPB-BOOK-251123/1691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escape some of its booking from data, allowing unauthenticated users to perform Stored Cross-Site Scripting attacks against administrators **CVE ID : CVE-2023-4620**		
Vendor: wpdevart					
Product: contact_form_builder					
Affected Version(s): * Up to (including) 2.1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in wpdevart Contact Form Builder, Contact Widget plugin <= 2.1.6 versions. **CVE ID : CVE-2023-46075**	N/A	A-WPD-CONT-251123/1692
Product: gallery					
Affected Version(s): * Up to (including) 2.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	6.1	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in wpdevart Gallery – Image and Video Gallery with Thumbnails plugin <= 2.0.3 versions. **CVE ID : CVE-2023-45630**	N/A	A-WPD-GALL-251123/1693
Vendor: wpdeveloper					
Product: essential_blocks					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 4.2.1					
Deserialization of Untrusted Data	20-Oct-2023	9.8	The Essential Blocks plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 4.2.0 via deserialization of untrusted input in the get_products function. This allows unauthenticated attackers to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code. **CVE ID : CVE-2023-4402**	N/A	A-WPD-ESSE-251123/1694
Affected Version(s): * Up to (including) 4.2.0					
Deserialization of Untrusted Data	20-Oct-2023	8.1	The Essential Blocks plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 4.2.0 via deserialization of untrusted input in the get_posts	N/A	A-WPD-ESSE-251123/1695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function. This allows unauthenticated attackers to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code. **CVE ID : CVE-2023-4386**		
Product: essential_blocks_pro					
Affected Version(s): * Up to (excluding) 1.1.1					
Deserialization of Untrusted Data	20-Oct-2023	9.8	The Essential Blocks plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 4.2.0 via deserialization of untrusted input in the get_products function. This allows unauthenticated attackers to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an	N/A	A-WPD-ESSE-251123/1696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code. **CVE ID : CVE-2023-4402**		
Vendor: wpdo					
Product: dologin_security					
Affected Version(s): * Up to (excluding) 3.7.1					
N/A	16-Oct-2023	6.5	The DoLogin Security WordPress plugin before 3.7.1 does not restrict the access of a widget that shows the IPs of failed logins to low privileged users. **CVE ID : CVE-2023-4800**	N/A	A-WPD-DOLO-251123/1697
Vendor: wpeka					
Product: wplegalpages					
Affected Version(s): * Up to (including) 2.9.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	4.8	The WPLegalPages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'wplegalpage' shortcode in versions up to, and including, 2.9.2 due to insufficient input sanitization	https://plugins.trac.wordpress.org/changeset/2976774/wplegalpages/trunk/public/class-wp-legal-pages-public.php#file0, https://plugins.trac.wordpress.org/browser/w	A-WPE-WPLE-251123/1698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and output escaping on user supplied attributes. This makes it possible for authenticated attackers with author-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-4968**	plegalpages/tags/2.9.2/public/class-wp-legal-pages-public.php#L150	
Vendor: wpexpertplugins					
Product: post_meta_data_manager					
Affected Version(s): * Up to (excluding) 1.2.1					
N/A	28-Oct-2023	8.8	The Post Meta Data Manager plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the pmdm_wp_change_user_meta and pmdm_wp_change_post_meta functions in versions up to, and including, 1.2.0. This makes it possible for authenticated attackers, with subscriber-level permissions and	https://plugins.trac.wordpress.org/changeset/2981559/post-meta-data-manager, https://www.wordfence.com/threat-intel/vulnerabilities/id/d7f4e710-99a2-49df-a513-725e1daaa18a?source=cve	A-WPE-POST-251123/1699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			above, to gain elevated (e.g., administrator) privileges. **CVE ID : CVE-2023-5425**		
N/A	28-Oct-2023	7.5	The Post Meta Data Manager plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the pmdm_wp_delete_user_meta, pmdm_wp_delete_term_meta, and pmdm_wp_ajax_delete_meta functions in versions up to, and including, 1.2.0. This makes it possible for unauthenticated attackers to delete user, term, and post meta belonging to arbitrary users. **CVE ID : CVE-2023-5426**	https://plugins.trac.wordpress.org/changeset/2981559/post-meta-data-manager, https://www.wordfence.com/threat-intel/vulnerabilities/id/d6a7f882-4582-4b08-9597-329d140ad782?source=cve	A-WPE-POST-251123/1700
Vendor: wpexperts					
Product: user_avatar-reloaded					
Affected Version(s): * Up to (excluding) 1.2.2					
N/A	16-Oct-2023	5.4	The User Avatar WordPress plugin before 1.2.2 does not properly sanitize and escape certain of its	N/A	A-WPE-USER-251123/1701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			shortcodes attributes, which could allow relatively low-privileged users like contributors to conduct Stored XSS attacks. **CVE ID : CVE-2023-4798**		
Vendor: wpfactory					
Product: ean_for_woocommerce					
Affected Version(s): * Up to (excluding) 6.1.0					
Missing Authorization	20-Oct-2023	4.3	The WooCommerce EAN Payment Gateway plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the refresh_order_ean_data AJAX action in versions up to 6.1.0. This makes it possible for authenticated attackers with contributor-level access and above, to update EAN numbers for orders. **CVE ID : CVE-2023-4947**	N/A	A-WPF-EAN_-251123/1702
Vendor: wpjohnny					
Product: comment_reply_email					
Affected Version(s): * Up to (including) 1.0.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPJohnny Comment Reply Email plugin <= 1.0.3 versions. **CVE ID : CVE-2023-45008**	N/A	A-WPJ-COMM-251123/1703
Vendor: wpknowledgebase					
Product: wp_knowledgebase					
Affected Version(s): * Up to (including) 1.3.4					
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Mihai Iova WordPress Knowledge base & Documentation Plugin – WP Knowledgebase plugin <= 1.3.4 versions. **CVE ID : CVE-2023-5802**	N/A	A-WPK-WP_K-251123/1704
Vendor: wpmet					
Product: wp_ultimate_review					
Affected Version(s): * Up to (including) 2.2.4					
Cross-Site Request Forgery (CSRF)	22-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Wpmet Wp Ultimate Review plugin <= 2.2.4 versions. **CVE ID : CVE-2023-46085**	N/A	A-WPM-WP_U-251123/1705
Vendor: wpmilitary					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wp_radio					
Affected Version(s): * Up to (including) 3.1.9					
Cross-Site Request Forgery (CSRF)	25-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WP Military WP Radio plugin <= 3.1.9 versions. **CVE ID : CVE-2023-46150**	N/A	A-WPM-WP_R-251123/1706
Vendor: wpmudev					
Product: defender_security					
Affected Version(s): * Up to (excluding) 4.1.0					
N/A	16-Oct-2023	5.3	The Defender Security WordPress plugin before 4.1.0 does not prevent redirects to the login page via the auth_redirect WordPress function, allowing an unauthenticated visitor to access the login page, even when the hide login page functionality of the plugin is enabled. **CVE ID : CVE-2023-5089**	N/A	A-WPM-DEFE-251123/1707
Vendor: wpvivid					
Product: migration\,_backup\,_staging					
Affected Version(s): * Up to (excluding) 0.9.90					
Improper Limitation of a Pathname to a	20-Oct-2023	6.5	The Migration, Backup, Staging – WPvivid plugin for WordPress is vulnerable to	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&repon	A-WPV-MIGR-251123/1708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			Directory Traversal in versions up to, and including, 0.9.89. This allows authenticated attackers with administrative privileges to delete the contents of arbitrary directories on the server, which can be a critical issue in a shared environments. **CVE ID : CVE-2023-4274**	ame=&new=2956458%40wpvivid-backuprestore%2Ftrunk&old=2948265%40wpvivid-backuprestore%2Ftrunk&sfp_email=&sfph_mail=	
Affected Version(s): * Up to (including) 0.9.89					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	4.8	The Migration, Backup, Staging – WPvivid plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the image file path parameter in versions up to, and including, 0.9.89 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	https://plugins.trac.wordpress.org/browser/wpvivid-backuprestore/tags/0.9.89/includes/upload-cleaner/class-wpvivid-uploads-cleaner.php#L161	A-WPV-MIGR-251123/1709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accesses an injected page. **CVE ID : CVE-2023-5120**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-2023	4.8	The Migration, Backup, Staging – WPvivid plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings (the backup path parameter) in versions up to, and including, 0.9.89 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-5121**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2956458%40wpvivid-backuprestore%2Ftrunk&old=2948265%40wpvivid-backuprestore%2Ftrunk&sfp_email=&sfph_mail=	A-WPV-MIGR-251123/1710
Affected Version(s): * Up to (including) 0.9.91					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Oct-2023	9.3	The Migration, Backup, Staging - WPvivid plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 0.9.91 via Google Drive API secrets stored in plaintext in the publicly visible plugin source. This could allow unauthenticated attackers to impersonate the WPVivid Google Drive account via the API if they can trick a user into reauthenticating via another vulnerability or social engineering. **CVE ID : CVE-2023-5576**	https://plugins.trac.wordpress.org/browser/wpvivid-backuprestore/tags/0.9.91/includes/customclass/client_secrets.json, https://plugins.trac.wordpress.org/changeset/2977863/	A-WPV-MIGR-251123/1711
Vendor: wpvnteam					
Product: wp_extra					
Affected Version(s): * Up to (excluding) 6.3					
Missing Authorization	25-Oct-2023	8.8	The WP EXtra plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the register() function	https://plugins.trac.wordpress.org/changeset/2977703/wp-extra, https://www.wordfence.com/threat-intel/vulnerabilities/id/87e3dd	A-WPV-WP_E-251123/1712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in versions up to, and including, 6.2. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to modify the contents of the .htaccess files located in a site's root directory or /wp-content and /wp-includes folders and achieve remote code execution. **CVE ID : CVE-2023-5311**	5e-0d77-4d78-8171-0beaf9482699?source=cve	
Vendor: wp_font_awesome_project					
Product: wp_font_awesome					
Affected Version(s): * Up to (including) 1.7.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	The WP Font Awesome plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 1.7.9 due to insufficient input sanitization and output escaping on 'icon' user supplied attribute. This makes it possible for authenticated attackers with contributor-level	https://plugins.trac.wordpress.org/browser/wp-font-awesome/trunk/wp-font-awesome.php?rev=2875119#L101, https://plugins.trac.wordpress.org/browser/wp-font-awesome/trunk/wp-font-awesome.php?rev=2875119#L68	A-WP_-WP_F-251123/1713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5127**		
Vendor: writercms					
Product: writercms					
Affected Version(s): 1.1.0					
Insufficiently Protected Credentials	26-Oct-2023	7.5	Incorrect access control in writercms v1.1.0 allows attackers to directly obtain backend account passwords via unspecified vectors. **CVE ID : CVE-2023-43905**	N/A	A-WRI-WRIT-251123/1714
Vendor: X.org					
Product: xwayland					
Affected Version(s): * Up to (excluding) 23.2.2					
Out-of-bounds Write	25-Oct-2023	7.8	A out-of-bounds write flaw was found in the xorg-x11-server. This issue occurs due to an incorrect calculation of a buffer offset when copying data stored in the heap in the XIChangeDeviceProperty function in Xi/xiproperty.c and	https://lists.x.org/archives/xorg-announce/2023-October/003430.html	A-X.O-XWAY-251123/1715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in RRChangeOutputProperty function in randr/rrproperty.c, allowing for possible escalation of privileges or denial of service. **CVE ID : CVE-2023-5367**		
Use After Free	25-Oct-2023	7	A use-after-free flaw was found in xorg-x11-server-Xvfb. This issue occurs in Xvfb with a very specific and legacy configuration (a multi-screen setup with multiple protocol screens, also known as Zaphod mode). If the pointer is warped from a screen 1 to a screen 0, a use-after-free issue may be triggered during shutdown or reset of the Xvfb server, allowing for possible escalation of privileges or denial of service. **CVE ID : CVE-2023-5574**	https://lists.x.org/archives/xorg-announce/2023-October/003430.html	A-X.O-XWAY-251123/1716
Use After Free	25-Oct-2023	4.7	A use-after-free flaw was found in the xorg-x11-server. An X server crash may occur in a very specific and	https://lists.x.org/archives/xorg-announce/2023-	A-X.O-XWAY-251123/1717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			legacy configuration (a multi-screen setup with multiple protocol screens, also known as Zaphod mode) if the pointer is warped from within a window on one screen to the root window of the other screen and if the original window is destroyed followed by another window being destroyed. **CVE ID : CVE-2023-5380**	October/003430.html	
Product: x_server					
Affected Version(s): * Up to (excluding) 21.1.9					
Out-of-bounds Write	25-Oct-2023	7.8	A out-of-bounds write flaw was found in the xorg-x11-server. This issue occurs due to an incorrect calculation of a buffer offset when copying data stored in the heap in the XIChangeDeviceProperty function in Xi/xiproperty.c and in RRChangeOutputProperty function in randr/rrproperty.c, allowing for possible escalation	https://lists.x.org/archives/xorg-announce/2023-October/003430.html	A-X.O-X_SE-251123/1718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privileges or denial of service. **CVE ID : CVE-2023-5367**		
Use After Free	25-Oct-2023	7	A use-after-free flaw was found in xorg-x11-server-Xvfb. This issue occurs in Xvfb with a very specific and legacy configuration (a multi-screen setup with multiple protocol screens, also known as Zaphod mode). If the pointer is warped from a screen 1 to a screen 0, a use-after-free issue may be triggered during shutdown or reset of the Xvfb server, allowing for possible escalation of privileges or denial of service. **CVE ID : CVE-2023-5574**	https://lists.x.org/archives/xorg-announce/2023-October/003430.html	A-X.O-X_SE-251123/1719
Use After Free	25-Oct-2023	4.7	A use-after-free flaw was found in the xorg-x11-server. An X server crash may occur in a very specific and legacy configuration (a multi-screen setup with multiple protocol screens, also known as	https://lists.x.org/archives/xorg-announce/2023-October/003430.html	A-X.O-X_SE-251123/1720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Zaphod mode) if the pointer is warped from within a window on one screen to the root window of the other screen and if the original window is destroyed followed by another window being destroyed. **CVE ID : CVE-2023-5380**		
Vendor: xgenecloud					
Product: nocodb					
Affected Version(s): 0.109.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Oct-2023	4.9	Nocodb is an open source Airtable alternative. Affected versions of nocodb contain a SQL injection vulnerability, that allows an authenticated attacker with creator access to query the underlying database. By supplying a specially crafted payload to the given an attacker can inject arbitrary SQL queries to be executed. Since this is a blind SQL injection, an attacker may need to use time-based	N/A	A-XGE-NOCO-251123/1721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payloads which would include a function to delay execution for a given number of seconds. The response time indicates, whether the result of the query execution was true or false. Depending on the result, the HTTP response will be returned after a given number of seconds, indicating TRUE, or immediately, indicating FALSE. In that way, an attacker can reveal the data present in the database. This vulnerability has been addressed in version 0.111.0. Users are advised to upgrade. There are no known workarounds for this vulnerability. This issue is also tracked as `GHSL-2023-141`. **CVE ID : CVE-2023-43794**		
Vendor: Xnview					
Product: nconvert					
Affected Version(s): 7.136					
Buffer Copy	18-Oct-2023	7.8	XNSoft Nconvert 7.136 is vulnerable	N/A	A-XNV-NCON-251123/1722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to Buffer Overflow. There is a User Mode Write AV via a crafted image file. Attackers could exploit this issue for a Denial of Service (DoS) or possibly to achieve code execution. **CVE ID : CVE-2023-43250**		
Improper Handling of Exceptional Conditions	19-Oct-2023	7.8	XNSoft Nconvert 7.136 has an Exception Handler Chain Corrupted via a crafted image file. Attackers could exploit this issue for a Denial of Service (DoS) or possibly to achieve code execution. **CVE ID : CVE-2023-43251**	N/A	A-XNV-NCON-251123/1723
Out-of-bounds Write	19-Oct-2023	7.8	XNSoft Nconvert 7.136 is vulnerable to Buffer Overflow via a crafted image file. **CVE ID : CVE-2023-43252**	N/A	A-XNV-NCON-251123/1724
Product: xnview					
Affected Version(s): 2.51.5					
Buffer Copy without Checking Size of Input ('Classic	27-Oct-2023	7.8	Buffer Overflow vulnerability in XnView Classic v.2.51.5 allows a local attacker to execute arbitrary	N/A	A-XNV-XNVI-251123/1725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			code via a crafted TIF file. **CVE ID : CVE-2023-46587**		
Vendor: xpand-it					
Product: write-back_manager					
Affected Version(s): 2.3.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Oct-2023	7.5	Xpand IT Write-back manager v2.3.1 allows attackers to perform a directory traversal via modification of the siteName parameter. **CVE ID : CVE-2023-27170**	N/A	A-XPA-WRIT-251123/1726
Vendor: xtendify					
Product: eonet_manual_user_approve					
Affected Version(s): * Up to (including) 2.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Alkaweb Eonet Manual User Approve plugin <= 2.1.3 versions. **CVE ID : CVE-2023-32738**	N/A	A-XTE-EONE-251123/1727
Product: simple_calendar					
Affected Version(s): * Up to (excluding) 3.2.6					
Cross-Site Request Forgery (CSRF)	25-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Simple Calendar – Google Calendar	N/A	A-XTE-SIMP-251123/1728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Plugin <= 3.2.5 versions. **CVE ID : CVE-2023-46189**		
Vendor: Xwiki					
Product: oauth_identity					
Affected Version(s): From (including) 1.0 Up to (excluding) 1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-2023	9.6	com.xwiki.identity-oauth:identity-oauth-ui is a package to aid in building identity and service providers based on OAuth authorizations. When a user logs in via the OAuth method, the identityOAuth parameters sent in the GET request is vulnerable to cross site scripting (XSS) and XWiki syntax injection. This allows remote code execution via the groovy macro and thus affects the confidentiality, integrity and availability of the whole XWiki installation. The issue has been fixed in Identity OAuth version 1.6. There are no known workarounds for this vulnerability	https://github.com/xwikisas/identity-oauth/commit/d805d3154b17c6bf455ddf5deb0a3461a3833bc6, https://github.com/xwikisas/identity-oauth/security/advisories/GHSA-h2rm-29ch-wfmh	A-XWI-OAUT-251123/1729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and users are advised to upgrade. **CVE ID : CVE-2023-45144**		
Product: Xwiki					
Affected Version(s): 7.2					
Improper Encoding or Escaping of Output	25-Oct-2023	8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In `org.xwiki.platform:xwiki-platform-web` versions 7.2-milestone-2 until 14.10.12 and `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.12 and 15.5-rc-1, it is possible to pass a title to the page creation action that isn't displayed at first but then executed in the second step. This can be used by an attacker to trick a victim to execute code, allowing script execution if the victim has script right or remote code execution including full access to the XWiki instance if the victim has programming right.	https://jira.xwiki.org/browse/XWIKI-20869, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-ghf6-2f42-mjh9, https://github.com/xwiki/xwiki-platform/commit/199e27ce7016757e66fa7cea99e718044a1b639b	A-XWI-XWIK-251123/1730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			For the attack to work, the attacker needs to convince the victim to visit a link like `<xwiki-host>/xwiki/bin/create/NonExistingSpace/WebHome?title=$services.logging.getLogger(%22foo%22).error(%22Script%20executed!%22)` where `<xwiki-host>` is the URL of the Wiki installation and to then click on the "Create" button on that page. The page looks like a regular XWiki page that the victim would also see when clicking the button to create a page that doesn't exist yet, the malicious code is not displayed anywhere on that page. After clicking the "Create" button, the malicious title would be displayed but at this point, the code has already been executed and the attacker could use this code also to hide the attack, e.g., by redirecting the victim again to the same page with an		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			innocent title. It thus seems plausible that this attack could work if the attacker can place a fake "create page" button on a page which is possible with edit right. This has been patched in `org.xwiki.platform:xwiki-platform-web` version 14.10.12 and `org.xwiki.platform:xwiki-platform-web-templates` versions 14.10.12 and 15.5-rc-1 by displaying the title already in the first step such that the victim can notice the attack before continuing. It is possible to manually patch the modified files from the patch in an existing installation. For the JavaScript change, the minified JavaScript file would need to be obtained from a build of XWiki and replaced accordingly. **CVE ID : CVE-2023-45135**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	9	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. `org.xwiki.platform:xwiki-platform-web` starting in version 3.1-milestone-1 and prior to 13.4-rc-1, `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.2 and 15.5-rc-1, and `org.xwiki.platform:xwiki-web-standard` starting in version 2.4-milestone-2 and prior to version 3.1-milestone-1 are vulnerable to cross-site scripting. An attacker can create a template provider on any document that is part of the wiki (could be the attacker's user profile) that contains malicious code. This code is executed when this template provider is selected during document creation which can be triggered by	https://github.com/xwiki/xwiki-platform/commit/ba56fda175156dd35035f2b8c86cbd8ef1f90c2e, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-gr82-8fj2-ggc3, https://jira.xwiki.org/browse/XWIKI-20962	A-XWI-XWIK-251123/1731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending the user to a URL. For the attacker, the only requirement is to have an account as by default the own user profile is editable. This allows an attacker to execute arbitrary actions with the rights of the user opening the malicious link. Depending on the rights of the user, this may allow remote code execution and full read and write access to the whole XWiki installation. This has been patched in `org.xwiki.platform:xwiki-platform-web` 13.4-rc-1, `org.xwiki.platform:xwiki-platform-web-templates` 14.10.2 and 15.5-rc-1, and `org.xwiki.platform:xwiki-web-standard` 3.1-milestone-1 by adding the appropriate escaping. The vulnerable template file createinline.vm is part of XWiki's WAR and can be		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patched by manually applying the changes from the fix. **CVE ID : CVE-2023-45134**		
Affected Version(s): 3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	9	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. `org.xwiki.platform:xwiki-platform-web` starting in version 3.1-milestone-1 and prior to 13.4-rc-1, `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.2 and 15.5-rc-1, and `org.xwiki.platform:xwiki-web-standard` starting in version 2.4-milestone-2 and prior to version 3.1-milestone-1 are vulnerable to cross-site scripting. An attacker can create a template provider on any document that is part of the wiki (could be the attacker's user profile) that contains malicious	https://github.com/xwiki/xwiki-platform/commit/ba56fda175156dd35035f2b8c86cbd8ef1f90c2e, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-gr82-8fj2-ggc3, https://jira.xwiki.org/browse/XWIKI-20962	A-XWI-XWIK-251123/1732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code. This code is executed when this template provider is selected during document creation which can be triggered by sending the user to a URL. For the attacker, the only requirement is to have an account as by default the own user profile is editable. This allows an attacker to execute arbitrary actions with the rights of the user opening the malicious link. Depending on the rights of the user, this may allow remote code execution and full read and write access to the whole XWiki installation. This has been patched in `org.xwiki.platform:xwiki-platform-web` 13.4-rc-1, `org.xwiki.platform:xwiki-platform-web-templates` 14.10.2 and 15.5-rc-1, and `org.xwiki.platform:xwiki-web-standard` 3.1-milestone-1 by adding the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			appropriate escaping. The vulnerable template file createinline.vm is part of XWiki's WAR and can be patched by manually applying the changes from the fix. **CVE ID : CVE-2023-45134**		
Affected Version(s): 15.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	9.6	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. When document names are validated according to a name strategy (disabled by default), XWiki starting in version 12.0-rc-1 and prior to versions 12.10.12 and 15.5-rc-1 is vulnerable to a reflected cross-site scripting attack in the page creation form. This allows an attacker to execute arbitrary actions with the rights of the user opening the malicious link. Depending on the rights of the user,	https://github.com/xwiki/xwiki-platform/commit/ba56fda175156dd35035f2b8c86cbd8ef1f90c2e, https://jira.xwiki.org/browse/XWIKI-20854, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-qcj9-gcpg-4w2w	A-XWI-XWIK-251123/1733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this may allow remote code execution and full read and write access to the whole XWiki installation. This has been patched in XWiki 14.10.12 and 15.5-rc-1 by adding appropriate escaping. The vulnerable template file `createinline.vm` is part of XWiki's WAR and can be patched by manually applying the changes from the fix. **CVE ID : CVE-2023-45136**		
Affected Version(s): 2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	9	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. `org.xwiki.platform:xwiki-platform-web` starting in version 3.1-milestone-1 and prior to 13.4-rc-1, `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.2 and 15.5-rc-1, and `org.xwiki.platform	https://github.com/xwiki/xwiki-platform/commit/ba56fda175156dd35035f2b8c86cbd8ef1f90c2e, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-gr82-8fj2-ggc3, https://jira.xwiki.org/browse/XWIKI-20962	A-XWI-XWIK-251123/1734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			:xwiki-web-standard` starting in version 2.4-milestone-2 and prior to version 3.1-milestone-1 are vulnerable to cross-site scripting. An attacker can create a template provider on any document that is part of the wiki (could be the attacker's user profile) that contains malicious code. This code is executed when this template provider is selected during document creation which can be triggered by sending the user to a URL. For the attacker, the only requirement is to have an account as by default the own user profile is editable. This allows an attacker to execute arbitrary actions with the rights of the user opening the malicious link. Depending on the rights of the user, this may allow remote code execution and full read and write		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to the whole XWiki installation. This has been patched in `org.xwiki.platform:xwiki-platform-web` 13.4-rc-1, `org.xwiki.platform:xwiki-platform-web-templates` 14.10.2 and 15.5-rc-1, and `org.xwiki.platform:xwiki-web-standard` 3.1-milestone-1 by adding the appropriate escaping. The vulnerable template file createinline.vm is part of XWiki's WAR and can be patched by manually applying the changes from the fix. **CVE ID : CVE-2023-45134**		
Affected Version(s): 3.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	9	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. `org.xwiki.platform:xwiki-platform-web` starting in version 3.1-milestone-1 and prior to 13.4-rc-1,	https://github.com/xwiki/xwiki-platform/commit/ba56fda175156dd35035f2b8c86cbd8ef1f90c2e, https://github.com/xwiki/xwiki-platform/securi	A-XWI-XWIK-251123/1735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.2 and 15.5-rc-1, and `org.xwiki.platform:xwiki-web-standard` starting in version 2.4-milestone-2 and prior to version 3.1-milestone-1 are vulnerable to cross-site scripting. An attacker can create a template provider on any document that is part of the wiki (could be the attacker's user profile) that contains malicious code. This code is executed when this template provider is selected during document creation which can be triggered by sending the user to a URL. For the attacker, the only requirement is to have an account as by default the own user profile is editable. This allows an attacker to execute arbitrary actions with the rights of the user opening	ty/advisories/GHSA-gr82-8fj2-ggc3, https://jira.xwiki.org/browse/XWIKI-20962	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the malicious link. Depending on the rights of the user, this may allow remote code execution and full read and write access to the whole XWiki installation. This has been patched in `org.xwiki.platform:xwiki-platform-web` 13.4-rc-1, `org.xwiki.platform:xwiki-platform-web-templates` 14.10.2 and 15.5-rc-1, and `org.xwiki.platform:xwiki-web-standard` 3.1-milestone-1 by adding the appropriate escaping. The vulnerable template file createinline.vm is part of XWiki's WAR and can be patched by manually applying the changes from the fix. **CVE ID : CVE-2023-45134**		
Affected Version(s): 3.1					
Improper Neutralization of Input During	25-Oct-2023	9	XWiki Platform is a generic wiki platform offering runtime services for applications	https://github.com/xwiki/xwiki-platform/commit/ba56fda1751	A-XWI-XWIK-251123/1736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			built on top of it. `org.xwiki.platform:xwiki-platform-web` starting in version 3.1-milestone-1 and prior to 13.4-rc-1, `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.2 and 15.5-rc-1, and `org.xwiki.platform:xwiki-web-standard` starting in version 2.4-milestone-2 and prior to version 3.1-milestone-1 are vulnerable to cross-site scripting. An attacker can create a template provider on any document that is part of the wiki (could be the attacker's user profile) that contains malicious code. This code is executed when this template provider is selected during document creation which can be triggered by sending the user to a URL. For the attacker, the only requirement is to have an account as by default the own	56dd35035f2b8c86cbd8ef1f90c2e, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-gr82-8fj2-ggc3, https://jira.xwiki.org/browse/XWIKI-20962	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user profile is editable. This allows an attacker to execute arbitrary actions with the rights of the user opening the malicious link. Depending on the rights of the user, this may allow remote code execution and full read and write access to the whole XWiki installation. This has been patched in `org.xwiki.platform:xwiki-platform-web` 13.4-rc-1, `org.xwiki.platform:xwiki-platform-web-templates` 14.10.2 and 15.5-rc-1, and `org.xwiki.platform:xwiki-web-standard` 3.1-milestone-1 by adding the appropriate escaping. The vulnerable template file createinline.vm is part of XWiki's WAR and can be patched by manually applying the changes from the fix.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45134		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. `org.xwiki.platform:xwiki-platform-web` starting in version 3.1-milestone-2 and prior to version 13.4-rc-1, as well as `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.12 and 15.5-rc-1, are vulnerable to cross-site scripting. When trying to create a document that already exists, XWiki displays an error message in the form for creating it. Due to missing escaping, this error message is vulnerable to raw HTML injection and thus XSS. The injected code is the document reference of the existing document so this requires that the attacker first creates a non-	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-93gh-jgjj-r929, https://jira.xwiki.org/browse/XWIKI-20961, https://github.com/xwiki/xwiki-platform/commit/ed8ec747967f8a16434806e727a57214a8843581	A-XWI-XWIK-251123/1737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			empty document whose name contains the attack code. This has been patched in `org.xwiki.platform:xwiki-platform-web` version 13.4-rc-1 and `org.xwiki.platform:xwiki-platform-web-templates` versions 14.10.12 and 15.5-rc-1 by adding the appropriate escaping. The vulnerable template file `createinline.vm` is part of XWiki's WAR and can be patched by manually applying the changes from the fix. **CVE ID : CVE-2023-45137**		
Affected Version(s): 9.4					
Exposure of Resource to Wrong Sphere	25-Oct-2023	6.5	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting in version 9.4-rc-1 and prior to versions 14.10.8 and 15.3-rc-1, when a document has been deleted and re-created, it is possible for users	https://github.com/xwiki/xwiki-platform/commit/f471f2a392aeeb9e51d59fdfe1d76fccf532523f, https://jira.xwiki.org/browse/XWIKI-20817, https://jira.xwiki.org/browse/XWIKI-20685,	A-XWI-XWIK-251123/1738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with view right on the re-created document but not on the deleted document to view the contents of the deleted document. Such a situation might arise when rights were added to the deleted document. This can be exploited through the diff feature and, partially, through the REST API by using versions such as `deleted:1` (where the number counts the deletions in the wiki and is thus guessable). Given sufficient rights, the attacker can also re-create the deleted document, thus extending the scope to any deleted document as long as the attacker has edit right in the location of the deleted document. This vulnerability has been patched in XWiki 14.10.8 and 15.3 RC1 by properly checking rights when deleted revisions of a document are	https://jira.xwiki.org/browse/XWIKI-20684	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accessed. The only workaround is to regularly clean deleted documents to minimize the potential exposure. Extra care should be taken when deleting sensitive documents that are protected individually (and not, e.g., by being placed in a protected space) or deleting a protected space as a whole. **CVE ID : CVE-2023-37911**		
Affected Version(s): From (excluding) 9.4 Up to (including) 14.10.8					
Exposure of Resource to Wrong Sphere	25-Oct-2023	6.5	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting in version 9.4-rc-1 and prior to versions 14.10.8 and 15.3-rc-1, when a document has been deleted and re-created, it is possible for users with view right on the re-created document but not on the deleted document to view the contents of the deleted document. Such a situation	https://github.com/xwiki/xwiki-platform/commit/f471f2a392aeeb9e51d59fdfe1d76fccf532523f, https://jira.xwiki.org/browse/XWIKI-20817, https://jira.xwiki.org/browse/XWIKI-20685, https://jira.xwiki.org/browse/XWIKI-20684	A-XWI-XWIK-251123/1739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			might arise when rights were added to the deleted document. This can be exploited through the diff feature and, partially, through the REST API by using versions such as `deleted:1` (where the number counts the deletions in the wiki and is thus guessable). Given sufficient rights, the attacker can also re-create the deleted document, thus extending the scope to any deleted document as long as the attacker has edit right in the location of the deleted document. This vulnerability has been patched in XWiki 14.10.8 and 15.3 RC1 by properly checking rights when deleted revisions of a document are accessed. The only workaround is to regularly clean deleted documents to minimize the potential exposure. Extra care should be taken when		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deleting sensitive documents that are protected individually (and not, e.g., by being placed in a protected space) or deleting a protected space as a whole. **CVE ID : CVE-2023-37911**		
Affected Version(s): From (including) 12.0 Up to (excluding) 14.10.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	9.6	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. When document names are validated according to a name strategy (disabled by default), XWiki starting in version 12.0-rc-1 and prior to versions 12.10.12 and 15.5-rc-1 is vulnerable to a reflected cross-site scripting attack in the page creation form. This allows an attacker to execute arbitrary actions with the rights of the user opening the malicious link. Depending on the rights of the user, this may allow	https://github.com/xwiki/xwiki-platform/commit/ba56fda175156dd35035f2b8c86cbd8ef1f90c2e, https://jira.xwiki.org/browse/XWIKI-20854, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-qcj9-gcpg-4w2w	A-XWI-XWIK-251123/1740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution and full read and write access to the whole XWiki installation. This has been patched in XWiki 14.10.12 and 15.5-rc-1 by adding appropriate escaping. The vulnerable template file `createinline.vm` is part of XWiki's WAR and can be patched by manually applying the changes from the fix. **CVE ID : CVE-2023-45136**		
Affected Version(s): From (including) 14.0 Up to (excluding) 14.10.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. `org.xwiki.platform:xwiki-platform-web` starting in version 3.1-milestone-2 and prior to version 13.4-rc-1, as well as `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.12 and 15.5-rc-1, are vulnerable	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-93gh-jgjj-r929, https://jira.xwiki.org/browse/XWIKI-20961, https://github.com/xwiki/xwiki-platform/commit/ed8ec747967f8a16434806e727a57214a8843581	A-XWI-XWIK-251123/1741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to cross-site scripting. When trying to create a document that already exists, XWiki displays an error message in the form for creating it. Due to missing escaping, this error message is vulnerable to raw HTML injection and thus XSS. The injected code is the document reference of the existing document so this requires that the attacker first creates a non-empty document whose name contains the attack code. This has been patched in `org.xwiki.platform:xwiki-platform-web` version 13.4-rc-1 and `org.xwiki.platform:xwiki-platform-web-templates` versions 14.10.12 and 15.5-rc-1 by adding the appropriate escaping. The vulnerable template file `createinline.vm` is part of XWiki's WAR and can be		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patched by manually applying the changes from the fix. **CVE ID : CVE-2023-45137**		
Affected Version(s): From (including) 14.0 Up to (excluding) 14.4.8					
Missing Authorization	25-Oct-2023	8.1	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting with the introduction of attachment move support in version 14.0-rc-1 and prior to versions 14.4.8, 14.10.4, and 15.0-rc-1, an attacker with edit access on any document (can be the user profile which is editable by default) can move any attachment of any other document to this attacker-controlled document. This allows the attacker to access and possibly publish any attachment of which the name is known, regardless if the attacker has view or edit rights on the source document of this attachment.	https://github.com/xwiki/xwiki-platform/commit/d7720219d60d7201c696c3196c9d4a86d0881325, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-rwwx-6572-mp29, https://jira.xwiki.org/browse/XWIKI-20334	A-XWI-XWIK-251123/1742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Further, the attachment is deleted from the source document. This vulnerability has been patched in XWiki 14.4.8, 14.10.4, and 15.0 RC1. There is no workaround apart from upgrading to a fixed version. **CVE ID : CVE-2023-37910**		
Affected Version(s): From (including) 14.10 Up to (excluding) 14.10.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	9	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. `org.xwiki.platform:xwiki-platform-web` starting in version 3.1-milestone-1 and prior to 13.4-rc-1, `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.2 and 15.5-rc-1, and `org.xwiki.platform:xwiki-web-standard` starting in version 2.4-milestone-2 and prior to version 3.1-milestone-1 are vulnerable to cross-site scripting. An attacker can	https://github.com/xwiki/xwiki-platform/commit/ba56fda175156dd35035f2b8c86cbd8ef1f90c2e, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-gr82-8fj2-ggc3, https://jira.xwiki.org/browse/XWIKI-20962	A-XWI-XWIK-251123/1743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			create a template provider on any document that is part of the wiki (could be the attacker's user profile) that contains malicious code. This code is executed when this template provider is selected during document creation which can be triggered by sending the user to a URL. For the attacker, the only requirement is to have an account as by default the own user profile is editable. This allows an attacker to execute arbitrary actions with the rights of the user opening the malicious link. Depending on the rights of the user, this may allow remote code execution and full read and write access to the whole XWiki installation. This has been patched in `org.xwiki.platform :xwiki-platform-web` 13.4-rc-1, `org.xwiki.platform :xwiki-platform-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-templates` 14.10.2 and 15.5-rc-1, and `org.xwiki.platform:xwiki-web-standard` 3.1-milestone-1 by adding the appropriate escaping. The vulnerable template file createinline.vm is part of XWiki's WAR and can be patched by manually applying the changes from the fix. **CVE ID : CVE-2023-45134**		
Affected Version(s): From (including) 14.5 Up to (excluding) 14.10.4					
Missing Authorization	25-Oct-2023	8.1	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting with the introduction of attachment move support in version 14.0-rc-1 and prior to versions 14.4.8, 14.10.4, and 15.0-rc-1, an attacker with edit access on any document (can be the user profile which is editable by default) can move any attachment of any	https://github.com/xwiki/xwiki-platform/commit/d7720219d60d7201c696c3196c9d4a86d0881325, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-rwwx-6572-mp29, https://jira.xwiki.org/browse/XWIKI-20334	A-XWI-XWIK-251123/1744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other document to this attacker-controlled document. This allows the attacker to access and possibly publish any attachment of which the name is known, regardless if the attacker has view or edit rights on the source document of this attachment. Further, the attachment is deleted from the source document. This vulnerability has been patched in XWiki 14.4.8, 14.10.4, and 15.0 RC1. There is no workaround apart from upgrading to a fixed version. **CVE ID : CVE-2023-37910**		
Affected Version(s): From (including) 15.0 Up to (excluding) 15.3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Oct-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting in version 3.5-milestone-1 and prior to versions 14.10.8 and 15.3-rc-1, triggering the office converter	https://jira.xwiki.org/browse/XWIKI-20715, https://github.com/xwiki/xwiki-platform/commit/45d182a4141ff22f3ff289cf71e4669bdc714544, https://github.com/xwiki/xwik	A-XWI-XWIK-251123/1745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with a specially crafted file name allows writing the attachment's content to an attacker-controlled location on the server as long as the Java process has write access to that location. In particular in the combination with attachment moving, a feature introduced in XWiki 14.0, this is easy to reproduce but it also possible to reproduce in versions as old as XWiki 3.5 by uploading the attachment through the REST API which doesn't remove `/` or `\` from the filename. As the mime type of the attachment doesn't matter for the exploitation, this could e.g., be used to replace the `jar`-file of an extension which would allow executing arbitrary Java code and thus impact the confidentiality, integrity and availability of the XWiki installation.	i-platform/security/advisories/GHSA-vcvr-v426-3m3m	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability has been patched in XWiki 14.10.8 and 15.3RC1. There are no known workarounds apart from disabling the office converter. **CVE ID : CVE-2023-37913**		
Affected Version(s): From (including) 15.0 Up to (excluding) 15.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	9.6	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. When document names are validated according to a name strategy (disabled by default), XWiki starting in version 12.0-rc-1 and prior to versions 12.10.12 and 15.5-rc-1 is vulnerable to a reflected cross-site scripting attack in the page creation form. This allows an attacker to execute arbitrary actions with the rights of the user opening the malicious link. Depending on the rights of the user, this may allow remote code execution and full	https://github.com/xwiki/xwiki-platform/commit/ba56fda175156dd35035f2b8c86cbd8ef1f90c2e, https://jira.xwiki.org/browse/XWIKI-20854, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-qcj9-gcpg-4w2w	A-XWI-XWIK-251123/1746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read and write access to the whole XWiki installation. This has been patched in XWiki 14.10.12 and 15.5-rc-1 by adding appropriate escaping. The vulnerable template file `createinline.vm` is part of XWiki's WAR and can be patched by manually applying the changes from the fix. **CVE ID : CVE-2023-45136**		
Improper Encoding or Escaping of Output	25-Oct-2023	8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In `org.xwiki.platform:xwiki-platform-web` versions 7.2-milestone-2 until 14.10.12 and `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.12 and 15.5-rc-1, it is possible to pass a title to the page creation action that isn't displayed at first but then executed in the second step.	https://jira.xwiki.org/browse/XWIKI-20869, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-ghf6-2f42-mjh9, https://github.com/xwiki/xwiki-platform/commit/199e27ce7016757e66fa7cea99e718044a1b639b	A-XWI-XWIK-251123/1747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This can be used by an attacker to trick a victim to execute code, allowing script execution if the victim has script right or remote code execution including full access to the XWiki instance if the victim has programming right. For the attack to work, the attacker needs to convince the victim to visit a link like `<xwiki-host>/xwiki/bin/create/NonExistingSpace/WebHome?title=$services.logging.getLogger(%22foo%22).error(%22Script%20executed!%22)` where `<xwiki-host>` is the URL of the Wiki installation and to then click on the "Create" button on that page. The page looks like a regular XWiki page that the victim would also see when clicking the button to create a page that doesn't exist yet, the malicious code is not displayed anywhere on that page. After clicking the "Create"		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			button, the malicious title would be displayed but at this point, the code has already been executed and the attacker could use this code also to hide the attack, e.g., by redirecting the victim again to the same page with an innocent title. It thus seems plausible that this attack could work if the attacker can place a fake "create page" button on a page which is possible with edit right. This has been patched in `org.xwiki.platform:xwiki-platform-web` version 14.10.12 and `org.xwiki.platform:xwiki-platform-web-templates` versions 14.10.12 and 15.5-rc-1 by displaying the title already in the first step such that the victim can notice the attack before continuing. It is possible to manually patch the modified files from the patch in an		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			existing installation. For the JavaScript change, the minified JavaScript file would need to be obtained from a build of XWiki and replaced accordingly. **CVE ID : CVE-2023-45135**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. `org.xwiki.platform:xwiki-platform-web` starting in version 3.1-milestone-2 and prior to version 13.4-rc-1, as well as `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.12 and 15.5-rc-1, are vulnerable to cross-site scripting. When trying to create a document that already exists, XWiki displays an error message in the form for creating it. Due to missing escaping, this error message	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-93gh-jgjj-r929, https://jira.xwiki.org/browse/XWIKI-20961, https://github.com/xwiki/xwiki-platform/commit/ed8ec747967f8a16434806e727a57214a8843581	A-XWI-XWIK-251123/1748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is vulnerable to raw HTML injection and thus XSS. The injected code is the document reference of the existing document so this requires that the attacker first creates a non-empty document whose name contains the attack code. This has been patched in `org.xwiki.platform:xwiki-platform-web` version 13.4-rc-1 and `org.xwiki.platform:xwiki-platform-web-templates` versions 14.10.12 and 15.5-rc-1 by adding the appropriate escaping. The vulnerable template file `createinline.vm` is part of XWiki's WAR and can be patched by manually applying the changes from the fix. **CVE ID : CVE-2023-45137**		
Affected Version(s): From (including) 3.1.1 Up to (excluding) 13.4					
Improper Neutralization of	25-Oct-2023	9	XWiki Platform is a generic wiki platform offering	https://github.com/xwiki/xwiki-	A-XWI-XWIK-251123/1749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			runtime services for applications built on top of it. `org.xwiki.platform:xwiki-platform-web` starting in version 3.1-milestone-1 and prior to 13.4-rc-1, `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.2 and 15.5-rc-1, and `org.xwiki.platform:xwiki-web-standard` starting in version 2.4-milestone-2 and prior to version 3.1-milestone-1 are vulnerable to cross-site scripting. An attacker can create a template provider on any document that is part of the wiki (could be the attacker's user profile) that contains malicious code. This code is executed when this template provider is selected during document creation which can be triggered by sending the user to a URL. For the attacker, the only requirement is to	platform/commit/ba56fda175156dd35035f2b8c86cbd8ef1f90c2e, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-gr82-8fj2-ggc3, https://jira.xwiki.org/browse/XWIKI-20962	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have an account as by default the own user profile is editable. This allows an attacker to execute arbitrary actions with the rights of the user opening the malicious link. Depending on the rights of the user, this may allow remote code execution and full read and write access to the whole XWiki installation. This has been patched in `org.xwiki.platform:xwiki-platform-web` 13.4-rc-1, `org.xwiki.platform:xwiki-platform-web-templates` 14.10.2 and 15.5-rc-1, and `org.xwiki.platform:xwiki-web-standard` 3.1-milestone-1 by adding the appropriate escaping. The vulnerable template file createinline.vm is part of XWiki's WAR and can be patched by manually applying the changes from the fix.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45134		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	5.4	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. `org.xwiki.platform:xwiki-platform-web` starting in version 3.1-milestone-2 and prior to version 13.4-rc-1, as well as `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.12 and 15.5-rc-1, are vulnerable to cross-site scripting. When trying to create a document that already exists, XWiki displays an error message in the form for creating it. Due to missing escaping, this error message is vulnerable to raw HTML injection and thus XSS. The injected code is the document reference of the existing document so this requires that the attacker first creates a non-	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-93gh-jgjj-r929, https://jira.xwiki.org/browse/XWIKI-20961, https://github.com/xwiki/xwiki-platform/commit/ed8ec747967f8a16434806e727a57214a8843581	A-XWI-XWIK-251123/1750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			empty document whose name contains the attack code. This has been patched in `org.xwiki.platform:xwiki-platform-web` version 13.4-rc-1 and `org.xwiki.platform:xwiki-platform-web-templates` versions 14.10.12 and 15.5-rc-1 by adding the appropriate escaping. The vulnerable template file `createinline.vm` is part of XWiki's WAR and can be patched by manually applying the changes from the fix. **CVE ID : CVE-2023-45137**		
Affected Version(s): From (including) 3.5 Up to (excluding) 14.10.8					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Oct-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting in version 3.5-milestone-1 and prior to versions 14.10.8 and 15.3-rc-1, triggering the office converter with a specially	https://jira.xwiki.org/browse/XWIKI-20715, https://github.com/xwiki/xwiki-platform/commit/45d182a4141ff22f3ff289cf71e4669bdc714544, https://github.com/xwiki/xwiki-	A-XWI-XWIK-251123/1751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted file name allows writing the attachment's content to an attacker-controlled location on the server as long as the Java process has write access to that location. In particular in the combination with attachment moving, a feature introduced in XWiki 14.0, this is easy to reproduce but it also possible to reproduce in versions as old as XWiki 3.5 by uploading the attachment through the REST API which doesn't remove `/` or `\` from the filename. As the mime type of the attachment doesn't matter for the exploitation, this could e.g., be used to replace the `jar`-file of an extension which would allow executing arbitrary Java code and thus impact the confidentiality, integrity and availability of the XWiki installation. This vulnerability	platform/security/advisories/GHSA-vcvr-v426-3m3m	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been patched in XWiki 14.10.8 and 15.3RC1. There are no known workarounds apart from disabling the office converter. **CVE ID : CVE-2023-37913**		
Affected Version(s): From (including) 5.1 Up to (excluding) 14.10.8					
Improper Control of Generation of Code ('Code Injection')	25-Oct-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting in version 5.1-rc-1 and prior to versions 14.10.8 and 15.3-rc-1, any user who can edit their own user profile can execute arbitrary script macros including Groovy and Python macros that allow remote code execution including unrestricted read and write access to all wiki contents. This has been patched in XWiki 14.10.8 and 15.3-rc-1 by adding proper escaping. As a workaround, the patch can be manually applied to the document `Menu.UIExtension Sheet`; only three	https://github.com/xwiki/xwiki-platform/commit/9e8f080094333dec63a8583229a3799208d773be, https://jira.xwiki.org/browse/XWIKI-20746, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-v2rr-xw95-wcjx	A-XWI-XWIK-251123/1752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lines need to be changed. **CVE ID : CVE-2023-37909**		
Affected Version(s): From (including) 7.3 Up to (excluding) 14.10.12					
Improper Encoding or Escaping of Output	25-Oct-2023	8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In `org.xwiki.platform:xwiki-platform-web` versions 7.2-milestone-2 until 14.10.12 and `org.xwiki.platform:xwiki-platform-web-templates` prior to versions 14.10.12 and 15.5-rc-1, it is possible to pass a title to the page creation action that isn't displayed at first but then executed in the second step. This can be used by an attacker to trick a victim to execute code, allowing script execution if the victim has script right or remote code execution including full access to the XWiki instance if the victim has programming right.	https://jira.xwiki.org/browse/XWIKI-20869, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-ghf6-2f42-mjh9, https://github.com/xwiki/xwiki-platform/commit/199e27ce7016757e66fa7cea99e718044a1b639b	A-XWI-XWIK-251123/1753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			For the attack to work, the attacker needs to convince the victim to visit a link like `<xwiki-host>/xwiki/bin/create/NonExistingSpace/WebHome?title=$services.logging.getLogger(%22foo%22).error(%22Script%20executed!%22)` where `<xwiki-host>` is the URL of the Wiki installation and to then click on the "Create" button on that page. The page looks like a regular XWiki page that the victim would also see when clicking the button to create a page that doesn't exist yet, the malicious code is not displayed anywhere on that page. After clicking the "Create" button, the malicious title would be displayed but at this point, the code has already been executed and the attacker could use this code also to hide the attack, e.g., by redirecting the victim again to the same page with an		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			innocent title. It thus seems plausible that this attack could work if the attacker can place a fake "create page" button on a page which is possible with edit right. This has been patched in `org.xwiki.platform:xwiki-platform-web` version 14.10.12 and `org.xwiki.platform:xwiki-platform-web-templates` versions 14.10.12 and 15.5-rc-1 by displaying the title already in the first step such that the victim can notice the attack before continuing. It is possible to manually patch the modified files from the patch in an existing installation. For the JavaScript change, the minified JavaScript file would need to be obtained from a build of XWiki and replaced accordingly. **CVE ID : CVE-2023-45135**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: xwiki-rendering					
Affected Version(s): * Up to (excluding) 14.10.6					
N/A	25-Oct-2023	8.8	XWiki Rendering is a generic Rendering system that converts textual input in a given syntax into another syntax. Prior to version 14.10.6 of `org.xwiki.platform:xwiki-core-rendering-macro-footnotes` and `org.xwiki.platform:xwiki-rendering-macro-footnotes` and prior to version 15.1-rc-1 of `org.xwiki.platform:xwiki-rendering-macro-footnotes`, the footnote macro executed its content in a potentially different context than the one in which it was defined. In particular in combination with the include macro, this allows privilege escalation from a simple user account in XWiki to programming rights and thus remote code execution,	https://github.com/xwiki/xwiki-rendering/security/advisories/GHSA-35j5-m29r-xfq5, https://jira.xwiki.org/browse/XRENDERING-688, https://github.com/xwiki/xwiki-rendering/commit/5f558b8fac8b716d19999225f38cb8ed0814116e	A-XWI-XWIK-251123/1754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacting the confidentiality, integrity and availability of the whole XWiki installation. This vulnerability has been patched in XWiki 14.10.6 and 15.1-rc-1. There is no workaround apart from upgrading to a fixed version of the footnote macro. **CVE ID : CVE-2023-37912**		
Affected Version(s): 15.0					
N/A	25-Oct-2023	8.8	XWiki Rendering is a generic Rendering system that converts textual input in a given syntax into another syntax. Prior to version 14.10.6 of `org.xwiki.platform:xwiki-core-rendering-macro-footnotes` and `org.xwiki.platform:xwiki-rendering-macro-footnotes` and prior to version 15.1-rc-1 of `org.xwiki.platform:xwiki-rendering-macro-footnotes`, the footnote macro executed its content in a	https://github.com/xwiki/xwiki-rendering/security/advisories/GHSA-35j5-m29r-xfq5, https://jira.xwiki.org/browse/XRENDERING-688, https://github.com/xwiki/xwiki-rendering/commit/5f558b8fac8b716d19999225f38cb8ed0814116e	A-XWI-XWIK-251123/1755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially different context than the one in which it was defined. In particular in combination with the include macro, this allows privilege escalation from a simple user account in XWiki to programming rights and thus remote code execution, impacting the confidentiality, integrity and availability of the whole XWiki installation. This vulnerability has been patched in XWiki 14.10.6 and 15.1-rc-1. There is no workaround apart from upgrading to a fixed version of the footnote macro. **CVE ID : CVE-2023-37912**		
Affected Version(s): From (including) 14.6 Up to (excluding) 14.10.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	9.6	XWiki Rendering is a generic Rendering system that converts textual input in a given syntax into another syntax. The cleaning of attributes during	https://github.com/xwiki/xwiki-rendering/security/advisories/GHSA-6gf5-c898-7rxp, https://jira.xwiki.org/browse/	A-XWI-XWIK-251123/1756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XHTML rendering, introduced in version 14.6-rc-1, allowed the injection of arbitrary HTML code and thus cross-site scripting via invalid attribute names. This can be exploited, e.g., via the link syntax in any content that supports XWiki syntax like comments in XWiki. When a user moves the mouse over a malicious link, the malicious JavaScript code is executed in the context of the user session. When this user is a privileged user who has programming rights, this allows server-side code execution with programming rights, impacting the confidentiality, integrity and availability of the XWiki instance. While this attribute was correctly recognized as not allowed, the attribute was still printed with a prefix `data-xwiki-	XRENDERING-697, https://github.com/xwiki/xwiki-rendering/commit/f4d5acac451dccaf276e69f0b49b72221eef5d2f	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			translated-attribute-` without further cleaning or validation. This problem has been patched in XWiki 14.10.4 and 15.0 RC1 by removing characters not allowed in data attributes and then validating the cleaned attribute again. There are no known workarounds apart from upgrading to a version including the fix. **CVE ID : CVE-2023-37908**		
Vendor: xxl-rpc_project					
Product: xxl-rpc					
Affected Version(s): * Up to (including) 1.7.0					
Deserialization of Untrusted Data	18-Oct-2023	10	XXL-RPC is a high performance, distributed RPC framework. With it, a TCP server can be set up using the Netty framework and the Hessian serialization mechanism. When such a configuration is used, attackers may be able to connect to the server and provide malicious serialized objects	N/A	A-XXL-XXL--251123/1757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that, once deserialized, force it to execute arbitrary code. This can be abused to take control of the machine the server is running by way of remote code execution. This issue has not been fixed. **CVE ID : CVE-2023-45146**		
Vendor: xydac					
Product: ultimate_taxonomy_manager					
Affected Version(s): * Up to (including) 2.0					
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in XYDAC Ultimate Taxonomy Manager plugin <= 2.0 versions. **CVE ID : CVE-2023-45836**	N/A	A-XYD-ULTI-251123/1758
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in XYDAC Ultimate Taxonomy Manager plugin <= 2.0 versions. **CVE ID : CVE-2023-45837**	N/A	A-XYD-ULTI-251123/1759
Vendor: ydb					
Product: ydb-go-sdk					
Affected Version(s): From (including) 3.48.6 Up to (excluding) 3.53.2					
Insertion of Sensitive	19-Oct-2023	5.5	ydb-go-sdk is a pure Go native and	https://github.com/ydb-	A-YDB-YDB--251123/1760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information into Log File			database/sql driver for the YDB platform. Since ydb-go-sdk v3.48.6 if you use a custom credentials object (implementation of interface Credentials it may leak into logs. This happens because this object could be serialized into an error message using `fmt.Errorf("something went wrong (credentials: %q)", credentials)` during connection to the YDB server. If such logging occurred, a malicious user with access to logs could read sensitive information (i.e. credentials) information and use it to get access to the database. ydb-go-sdk contains this problem in versions from v3.48.6 to v3.53.2. The fix for this problem has been released in version v3.53.3. Users are advised to upgrade. Users unable to upgrade should implement the	platform/ydb-go-sdk/security/advisories/GHSA-q24m-6h38-5xj8	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`fmt.Stringer` interface in your custom credentials type with explicit stringify of object state. **CVE ID : CVE-2023-45825**		
Vendor: yettiesoft					
Product: vestcert					
Affected Version(s): From (including) 2.3.6 Up to (excluding) 2.5.30					
Inclusion of Functionality from Untrusted Control Sphere	30-Oct-2023	9.8	In Yettiesoft VestCert versions 2.36 to 2.5.29, a vulnerability exists due to improper validation of third-party modules. This allows malicious actors to load arbitrary third-party modules, leading to remote code execution. **CVE ID : CVE-2023-45798**	N/A	A-YET-VEST-251123/1761
Vendor: zanllp					
Product: stable_diffusion_webui_infinite_image_browsing					
Affected Version(s): * Up to (excluding) 5.0					
N/A	22-Oct-2023	7.5	The zanllp sd-webui-infinite-image-browsing (aka Infinite Image Browsing) extension before 977815a for stable-diffusion-webui (aka Stable Diffusion web UI), if Gradio	https://github.com/zanllp/sd-webui-infinite-image-browsing/pull/368/commits/977815a2b28ad953c10ef0114c365f698c4b8f19, https://github.c	A-ZAN-STAB-251123/1762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication is enabled without secret key configuration, allows remote attackers to read any local file via /file?path= in the URL, as demonstrated by reading /proc/self/environ to discover credentials. **CVE ID : CVE-2023-46315**	om/zanllp/sd-webui-infinite-image-browsing/issues/387	
Vendor: zaytech					
Product: smart_online_order_for_clover					
Affected Version(s): * Up to (excluding) 1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Oct-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Zaytech Smart Online Order for Clover plugin <= 1.5.4 versions. **CVE ID : CVE-2023-46312**	N/A	A-ZAY-SMAR-251123/1763
Vendor: zchunk					
Product: zchunk					
Affected Version(s): * Up to (excluding) 1.3.2					
Integer Overflow or Wraparound	19-Oct-2023	7.8	zchunk before 1.3.2 has multiple integer overflows via malformed zchunk files to lib/comp/comp.c, lib/comp/zstd/zstd.c,	https://bugzilla.suse.com/show_bug.cgi?id=1216268, https://github.com/zchunk/zchunk/commit/08aec2b4dfd7f709b6e3d511411ffcc83ed4efbe,	A-ZCH-ZCHU-251123/1764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lib/dl/multipart.c, or lib/header.c. **CVE ID : CVE-2023-46228**	https://github.com/zchunk/zchunk/compare/1.3.1...1.3.2	
Vendor: zentao					
Product: biz					
Affected Version(s): * Up to (including) 4.1.3					
Cross-Site Request Forgery (CSRF)	27-Oct-2023	8.8	ZenTao Biz version 4.1.3 and before is vulnerable to Cross Site Request Forgery (CSRF). **CVE ID : CVE-2023-46375**	N/A	A-ZEN-BIZ-251123/1765
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	6.1	ZenTao Enterprise Edition version 4.1.3 and before is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-46374**	N/A	A-ZEN-BIZ-251123/1766
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-2023	6.1	ZenTao Biz version 4.1.3 and before has a Cross Site Scripting (XSS) vulnerability in the Version Library. **CVE ID : CVE-2023-46491**	N/A	A-ZEN-BIZ-251123/1767
Affected Version(s): * Up to (including) 8.7					
Cleartext Storage of Sensitive Information	27-Oct-2023	7.5	Zentao Biz version 8.7 and before is vulnerable to Information Disclosure. **CVE ID : CVE-2023-46376**	N/A	A-ZEN-BIZ-251123/1768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: zitadel					
Product: zitadel					
Affected Version(s): * Up to (excluding) 2.38.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2023	5.4	ZITADEL is an identity infrastructure management system. ZITADEL users can upload their own avatar image using various image types including SVG. SVG can include scripts, such as javascript, which can be executed during rendering. Due to a missing security header, an attacker could inject code to an SVG to gain access to the victim's account in certain scenarios. A victim would need to directly open the malicious image in the browser, where a single session in ZITADEL needs to be active for this exploit to work. If the possible victim had multiple or no active sessions in ZITADEL, the attack would not succeed. This issue has been patched in version 2.39.2 and 2.38.2.	https://github.com/zitadel/zitadel/releases/tag/v2.39.2, https://github.com/zitadel/zitadel/releases/tag/v2.38.2, https://github.com/zitadel/zitadel/security/advisories/GHSA-954h-jrpm-72pm	A-ZIT-ZITA-251123/1769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46238		
Affected Version(s): From (including) 2.39.0 Up to (excluding) 2.39.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2023	5.4	ZITADEL is an identity infrastructure management system. ZITADEL users can upload their own avatar image using various image types including SVG. SVG can include scripts, such as javascript, which can be executed during rendering. Due to a missing security header, an attacker could inject code to an SVG to gain access to the victim's account in certain scenarios. A victim would need to directly open the malicious image in the browser, where a single session in ZITADEL needs to be active for this exploit to work. If the possible victim had multiple or no active sessions in ZITADEL, the attack would not succeed. This issue has been patched in version 2.39.2 and 2.38.2.	https://github.com/zitadel/zitadel/releases/tag/v2.39.2, https://github.com/zitadel/zitadel/releases/tag/v2.38.2, https://github.com/zitadel/zitadel/security/advisories/GHSA-954h-jrpm-72pm	A-ZIT-ZITA-251123/1770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46238		
Vendor: zscaler					
Product: client_connector					
Affected Version(s): * Up to (excluding) 4.1					
Improper Link Resolution Before File Access ('Link Following')	23-Oct-2023	7.3	Zscaler Client Connector for Windows before 4.1 writes/deletes a configuration file inside specific folders on the disk. A malicious user can replace the folder and execute code as a privileged user. **CVE ID : CVE-2023-28797**	N/A	A-ZSC-CLIE-251123/1771
Affected Version(s): * Up to (excluding) 1.3.1.6					
Out-of-bounds Write	23-Oct-2023	7.8	Buffer overflow vulnerability in the signelf library used by Zscaler Client Connector on Linux allows Code Injection. This issue affects Zscaler Client Connector for Linux: before 1.3.1.6. **CVE ID : CVE-2023-28793**	N/A	A-ZSC-CLIE-251123/1772
Origin Validation Error	23-Oct-2023	7.8	Origin Validation Error vulnerability in Zscaler Client Connector on Linux allows Inclusion of Code in Existing Process. This issue	N/A	A-ZSC-CLIE-251123/1773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Zscaler Client Connector for Linux: before 1.3.1.6. **CVE ID : CVE-2023-28795**		
Improper Verification of Cryptographic Signature	23-Oct-2023	7.8	Improper Verification of Cryptographic Signature vulnerability in Zscaler Client Connector on Linux allows Code Injection. This issue affects Zscaler Client Connector for Linux: before 1.3.1.6. **CVE ID : CVE-2023-28796**	N/A	A-ZSC-CLIE-251123/1774
Affected Version(s): * Up to (excluding) 1.4.0.105					
N/A	23-Oct-2023	9.8	An Improper Input Validation vulnerability in Zscaler Client Connector on Linux allows Privilege Escalation. This issue affects Client Connector: before 1.4.0.105 **CVE ID : CVE-2023-28805**	N/A	A-ZSC-CLIE-251123/1775
Improper Verification of Cryptographic Signature	23-Oct-2023	5.3	An Improper Verification of Cryptographic Signature vulnerability in Zscaler Client Connector on Linux	N/A	A-ZSC-CLIE-251123/1776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows replacing binaries.This issue affects Linux Client Connector: before 1.4.0.105 **CVE ID : CVE-2023-28804**		
Affected Version(s): * Up to (excluding) 3.9					
Authentication Bypass by Spoofing	23-Oct-2023	6.5	An authentication bypass by spoofing of a device with a synthetic IP address is possible in Zscaler Client Connector on Windows, allowing a functionality bypass. This issue affects Client Connector: before 3.9. **CVE ID : CVE-2023-28803**	N/A	A-ZSC-CLIE-251123/1777
Vendor: zzzcms					
Product: zzzcms					
Affected Version(s): 2.1.9					
Unrestricted Upload of File with Dangerous Type	25-Oct-2023	9.8	File Upload vulnerability in zzzCMS v.2.1.9 allows a remote attacker to execute arbitrary code via modification of the imageext parameter from jpg, jpeg,gif, and png to jpg, jpeg,gif, png, pphphp. **CVE ID : CVE-2023-45554**	N/A	A-ZZZ-ZZZC-251123/1778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	25-Oct-2023	7.8	File Upload vulnerability in zzzCMS v.2.1.9 allows a remote attacker to execute arbitrary code via a crafted file to the down_url function in zzz.php file. **CVE ID : CVE-2023-45555**	N/A	A-ZZZ-ZZZC-251123/1779
Product: zzzphp					
Affected Version(s): 2.2.0					
URL Redirection to Untrusted Site ('Open Redirect')	18-Oct-2023	6.1	zzzcms v2.2.0 was discovered to contain an open redirect vulnerability. **CVE ID : CVE-2023-45909**	https://github.com/Num-Nine/CVE/issues/7	A-ZZZ-ZZZP-251123/1780
Hardware					
Vendor: airtel					
Product: dragon_path_707gr1					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2023	4.8	A vulnerability classified as problematic has been found in Dragon Path 707GR1 up to 20231022. Affected is an unknown function of the component Ping Diagnostics. The manipulation of the argument Host Address with the input >><img/src/onerror=alert(1)> leads	N/A	H-AIR-DRAG-281123/1781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-243594 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-5789**		
Vendor: AMD					
Product: radeon_pro_w5500					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1782
Product: radeon_pro_w5700					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD	https://www.amd.com/en/corporate/product-	H-AMD-RADE-281123/1783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	security/bulletin/AMD-SB-6009	
Product: radeon_pro_w6300					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1784
Product: radeon_pro_w6400					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics	https://www.amd.com/en/corporate/product-security/bulleti	H-AMD-RADE-281123/1785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	n/AMD-SB-6009	
Product: radeon_pro_w6600					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1786
Product: radeon_pro_w6800					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow	https://www.amd.com/en/corporate/product-security/bulleti	H-AMD-RADE-281123/1787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	n/AMD-SB-6009	
Product: radeon_pro_w7500					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1788
Product: radeon_pro_w7600					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_pro_w7800					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1790
Product: radeon_pro_w7900					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_5300					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1792
Product: radeon_rx_5300m					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_5300_xt					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1794
Product: radeon_rx_5500					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_5500m					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1796
Product: radeon_rx_5500_xt					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_5600					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1798
Product: radeon_rx_5600m					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_5600_xt					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1800
Product: radeon_rx_5700					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_5700m					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1802
Product: radeon_rx_5700_xt					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_6300m					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1804
Product: radeon_rx_6400					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_6450m					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1806
Product: radeon_rx_6500m					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_6500_xt					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1808
Product: radeon_rx_6550m					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_6550s					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1810
Product: radeon_rx_6600					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_6600m					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1812
Product: radeon_rx_6600s					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_6600_xt					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1814
Product: radeon_rx_6650m					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_6650m_xt					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1816
Product: radeon_rx_6650_xt					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_6700					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1818
Product: radeon_rx_6700m					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_6700s					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1820
Product: radeon_rx_6700_xt					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_6750_gre_10gb					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1822
Product: radeon_rx_6750_gre_12gb					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_6750_xt					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1824
Product: radeon_rx_6800					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_6800s					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1826
Product: radeon_rx_6800_xt					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_6900_xt					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1828
Product: radeon_rx_6950_xt					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_7600					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1830
Product: radeon_rx_7600m					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_7600m_xt					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1832
Product: radeon_rx_7600s					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_7700s					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1834
Product: radeon_rx_7700_xt					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_7800_xt					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1836
Product: radeon_rx_7900m					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_7900_gre					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1838
Product: radeon_rx_7900_xt					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: radeon_rx_7900_xtx					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RADE-281123/1840
Product: ryzen_3_7320u					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_3_7335u					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1842
Product: ryzen_3_7440u					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_5_6600h					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1844
Product: ryzen_5_6600hs					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_5_6600u					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1846
Product: ryzen_5_7500f					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_5_7520u					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1848
Product: ryzen_5_7535hs					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_5_7535u					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1850
Product: ryzen_5_7540u					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_5_7600					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1852
Product: ryzen_5_7600x					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_5_7640h					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1854
Product: ryzen_5_7640u					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_5_7645hx					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1856
Product: ryzen_5_pro_7640hs					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_5_pro_7645					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1858
Product: ryzen_7_6800h					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_7_6800hs					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1860
Product: ryzen_7_6800u					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_7_7700					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1862
Product: ryzen_7_7700x					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_7_7735hs					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1864
Product: ryzen_7_7735u					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_7_7736u					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1866
Product: ryzen_7_7745hx					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_7_7800x3d					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1868
Product: ryzen_7_7840h					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_7_7840u					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1870
Product: ryzen_7_pro_7745					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_7_pro_7840hs					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1872
Product: ryzen_9_6900hs					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_9_6900hx					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1874
Product: ryzen_9_6980hs					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_9_6980hx					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1876
Product: ryzen_9_7845hx					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_9_7900					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1878
Product: ryzen_9_7900x					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_9_7900x3d					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1880
Product: ryzen_9_7940h					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_9_7945hx					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1882
Product: ryzen_9_7945hx3d					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_9_7950x					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1884
Product: ryzen_9_7950x3d					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Product: ryzen_9_pro_7940hs					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution. **CVE ID : CVE-2023-20598**	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1886
Product: ryzen_9_pro_7945					
Affected Version(s): -					
N/A	17-Oct-2023	7.8	An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a	https://www.amd.com/en/corporate/product-security/bulletin/AMD-SB-6009	H-AMD-RYZE-281123/1887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential arbitrary code execution. **CVE ID : CVE-2023-20598**		
Vendor: Axis					
Product: a8207-ve_mk_ii					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-A820-281123/1888
Product: m3215					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis	https://www.axis.com/dam/public/45/3c/a1/cve-2023-	H-AXI-M321-281123/1889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	21414pdf-en-US-412758.pdf	
Product: m3216					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-M321-281123/1890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**		
Product: m4317-plve					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-M431-281123/1891
Product: m4318-plve					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during	https://www.axis.com/dam/pu	H-AXI-M431-281123/1892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	blic/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	
Product: m4327-p					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection.	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-M432-281123/1893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**		
Product: m4328-p					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-M432-281123/1894
Product: p1467-le					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-P146-281123/1895
Product: p1468-le					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-P146-281123/1896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**		
Product: p1468-xle					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-P146-281123/1897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21414		
Product: p3265-lv					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-P326-281123/1898
Product: p3265-lve					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-P326-281123/1899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**		
Product: p3265-v					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-P326-281123/1900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information and solution. **CVE ID : CVE-2023-21414**		
Product: p3267-lv					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-P326-281123/1901
Product: p3267-lve					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications.	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-P326-281123/1902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**		
Product: p3268-lv					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw.	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-P326-281123/1903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**		
Product: p3268-lve					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-P326-281123/1904
Product: p3827-pve					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal	https://www.axis.com/dam/public/45/3c/a1/	H-AXI-P382-281123/1905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	cve-2023-21414pdf-en-US-412758.pdf	
Product: p4705-plve					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-P470-281123/1906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**		
Product: p4707-plve					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-P470-281123/1907
Product: q1656					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-Q165-281123/1908
Product: q1656-b					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-Q165-281123/1909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**		
Product: q1656-be					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-Q165-281123/1910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: q1656-ble					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-Q165-281123/1911
Product: q1656-dle					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-Q165-281123/1912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**		
Product: q1656-le					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-Q165-281123/1913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information and solution. **CVE ID : CVE-2023-21414**		
Product: q1961-te					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-Q196-281123/1914
Product: q2101-te					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications.	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-Q210-281123/1915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**		
Product: q3527-lve					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw.	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-Q352-281123/1916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**		
Product: q3536-lve					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-Q353-281123/1917
Product: q3538-lve					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal	https://www.axis.com/dam/public/45/3c/a1/	H-AXI-Q353-281123/1918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	cve-2023-21414pdf-en-US-412758.pdf	
Product: q3626-ve					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-Q362-281123/1919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**		
Product: q3628-ve					
Affected Version(s): -					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-Q362-281123/1920
Product: xfq1656					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	H-AXI-XFQ1-281123/1921
Vendor: bakerhughes					
Product: bentley_nevada_3500_system					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	19-Oct-2023	8.2	Baker Hughes – Bently Nevada 3500 System TDI Firmware version 5.05 contains a cleartext transmission vulnerability which could allow an attacker to steal the authentication	N/A	H-BAK-BENT-281123/1922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			secret from communication traffic to the device and reuse it for arbitrary requests. **CVE ID : CVE-2023-34441**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2023	7.5	Baker Hughes – Bently Nevada 3500 System TDI Firmware version 5.05 contains a vulnerability in their password retrieval functionality which could allow an attacker to access passwords stored on the device. **CVE ID : CVE-2023-34437**	N/A	H-BAK-BENT-281123/1923
Authentication Bypass by Capture-replay	19-Oct-2023	6.5	Baker Hughes – Bently Nevada 3500 System TDI Firmware version 5.05 contains a replay vulnerability which could allow an attacker to replay older captured packets of traffic to the device to gain access. **CVE ID : CVE-2023-36857**	N/A	H-BAK-BENT-281123/1924
Vendor: boschrexroth					
Product: ctrlx_hmi_web_panel_wr2107					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Missing Authentication for Critical Function	25-Oct-2023	8.8	The vulnerability allows an unprivileged user with access to the subnet of the TPC-110W device to gain a root shell on the device itself abusing the lack of authentication of the 'su' binary file installed on the device that can be accessed through the ADB (Android Debug Bridge) protocol exposed on the network. **CVE ID : CVE-2023-41255**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1925
Missing Authentication for Critical Function	25-Oct-2023	8.8	The Android Client application, when enrolled with the define method 1(the user manually inserts the server ip address), use HTTP protocol to retrieve sensitive information (ip address and credentials to connect to a remote MQTT broker entity) instead of HTTPS and this feature is not configurable by the user.	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45220		
Cleartext Transmission of Sensitive Information	25-Oct-2023	8.8	The Android Client application, when enrolled with the define method 1 (the user manually inserts the server ip address), use HTTP protocol to retrieve sensitive information (ip address and credentials to connect to a remote MQTT broker entity) instead of HTTPS and this feature is not configurable by the user. Due to the lack of encryption of HTTP,this issue allows an attacker placed in the same subnet network of the HMI device to intercept username and password necessary to authenticate to the MQTT server responsible to implement the remote management protocol. **CVE ID : CVE-2023-45321**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1927
Missing Authentication for	25-Oct-2023	8.8	The Android Client application, when enrolled to the AppHub	https://psirt.bosch.com/security-advisories/BOS	H-BOS-CTRL-281123/1928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			server,connects to an MQTT broker without enforcing any server authentication. This issue allows an attacker to force the Android Client application to connect to a malicious MQTT broker, enabling it to send fake messages to the HMI device **CVE ID : CVE-2023-45851**	CH-SA-175607.html	
Use of Hard-coded Credentials	25-Oct-2023	8.8	The Android Client application, when enrolled to the AppHub server, connects to an MQTT broker to exchange messages and receive commands to execute on the HMI device. The protocol builds on top of MQTT to implement the remote management of the device is encrypted with a hard-coded DES symmetric key, that can be retrieved reversing both the Android Client application and the server-side web application.	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue allows an attacker able to control a malicious MQTT broker on the same subnet network of the device, to craft malicious messages and send them to the HMI device, executing arbitrary commands on the device itself. **CVE ID : CVE-2023-46102**		
Use of Hard-coded Credentials	25-Oct-2023	7.8	The vulnerability allows an unprivileged (untrusted) third-party application to arbitrary modify the server settings of the Android Client application, inducing it to connect to an attacker - controlled malicious server.This is possible by forging a valid broadcast intent encrypted with a hardcoded RSA key pair **CVE ID : CVE-2023-41372**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1930
Missing Authorization	25-Oct-2023	7.8	The vulnerability allows a low privileged	https://psirt.bosch.com/security-advisories/BOS	H-BOS-CTRL-281123/1931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(untrusted) application to modify a critical system property that should be denied, in order to enable the ADB (Android Debug Bridge) protocol to be exposed on the network, exploiting it to gain a privileged shell on the device without requiring the physical access through USB. **CVE ID : CVE-2023-43488**	CH-SA-175607.html	
N/A	25-Oct-2023	6.8	The vulnerability allows a low privileged user that have access to the device when locked in Kiosk mode to install an arbitrary Android application and leverage it to have access to critical device settings such as the device power management or eventually the device secure settings (ADB debug). **CVE ID : CVE-2023-45844**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1932
N/A	25-Oct-2023	3.3	The vulnerability allows an	https://psirt.bosch.com/securit	H-BOS-CTRL-281123/1933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unprivileged(untrusted) third-party application to interact with a content-provider unsafely exposed by the Android Agent application, potentially modifying sensitive settings of the Android Client application itself. **CVE ID : CVE-2023-41960**	y-advisories/BOSCH-SA-175607.html	
Product: ctrlx_hmi_web_panel_wr2110					
Affected Version(s): -					
Missing Authentication for Critical Function	25-Oct-2023	8.8	The vulnerability allows an unprivileged user with access to the subnet of the TPC-110W device to gain a root shell on the device itself abusing the lack of authentication of the 'su' binary file installed on the device that can be accessed through the ADB (Android Debug Bridge) protocol exposed on the network. **CVE ID : CVE-2023-41255**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1934
Missing Authentication for	25-Oct-2023	8.8	The Android Client application, when enrolled with the define method 1(the user	https://psirt.bosch.com/security-advisories/BOS	H-BOS-CTRL-281123/1935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			manually inserts the server ip address), use HTTP protocol to retrieve sensitive information (ip address and credentials to connect to a remote MQTT broker entity) instead of HTTPS and this feature is not configurable by the user. **CVE ID : CVE-2023-45220**	CH-SA-175607.html	
Cleartext Transmission of Sensitive Information	25-Oct-2023	8.8	The Android Client application, when enrolled with the define method 1 (the user manually inserts the server ip address), use HTTP protocol to retrieve sensitive information (ip address and credentials to connect to a remote MQTT broker entity) instead of HTTPS and this feature is not configurable by the user. Due to the lack of encryption of HTTP,this issue allows an attacker placed in the same subnet network of the HMI device to intercept username	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and password necessary to authenticate to the MQTT server responsible to implement the remote management protocol. **CVE ID : CVE-2023-45321**		
Missing Authentication for Critical Function	25-Oct-2023	8.8	The Android Client application, when enrolled to the AppHub server,connects to an MQTT broker without enforcing any server authentication. This issue allows an attacker to force the Android Client application to connect to a malicious MQTT broker, enabling it to send fake messages to the HMI device **CVE ID : CVE-2023-45851**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1937
Use of Hard-coded Credentials	25-Oct-2023	8.8	The Android Client application, when enrolled to the AppHub server, connects to an MQTT broker to exchange messages and receive commands	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute on the HMI device. The protocol builds on top of MQTT to implement the remote management of the device is encrypted with a hard-coded DES symmetric key, that can be retrieved reversing both the Android Client application and the server-side web application. This issue allows an attacker able to control a malicious MQTT broker on the same subnet network of the device, to craft malicious messages and send them to the HMI device, executing arbitrary commands on the device itself. **CVE ID : CVE-2023-46102**		
Use of Hard-coded Credentials	25-Oct-2023	7.8	The vulnerability allows an unprivileged (untrusted) third-party application to arbitrary modify the server settings of the Android Client application, inducing it to	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connect to an attacker - controlled malicious server.This is possible by forging a valid broadcast intent encrypted with a hardcoded RSA key pair **CVE ID : CVE-2023-41372**		
Missing Authorization	25-Oct-2023	7.8	The vulnerability allows a low privileged (untrusted) application to modify a critical system property that should be denied, in order to enable the ADB (Android Debug Bridge) protocol to be exposed on the network, exploiting it to gain a privileged shell on the device without requiring the physical access through USB. **CVE ID : CVE-2023-43488**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1940
N/A	25-Oct-2023	6.8	The vulnerability allows a low privileged user that have access to the device when locked in Kiosk mode to install an arbitrary Android	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application and leverage it to have access to critical device settings such as the device power management or eventually the device secure settings (ADB debug). **CVE ID : CVE-2023-45844**		
N/A	25-Oct-2023	3.3	The vulnerability allows an unprivileged(untrusted) third-party application to interact with a content-provider unsafely exposed by the Android Agent application, potentially modifying sensitive settings of the Android Client application itself. **CVE ID : CVE-2023-41960**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1942
Product: ctrlx_hmi_web_panel_wr2115					
Affected Version(s): -					
Missing Authentication for Critical Function	25-Oct-2023	8.8	The vulnerability allows an unprivileged user with access to the subnet of the TPC-110W device to gain a root shell on the device itself abusing the lack of authentication	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the 'su' binary file installed on the device that can be accessed through the ADB (Android Debug Bridge) protocol exposed on the network. **CVE ID : CVE-2023-41255**		
Missing Authentication for Critical Function	25-Oct-2023	8.8	The Android Client application, when enrolled with the define method 1(the user manually inserts the server ip address), use HTTP protocol to retrieve sensitive information (ip address and credentials to connect to a remote MQTT broker entity) instead of HTTPS and this feature is not configurable by the user. **CVE ID : CVE-2023-45220**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1944
Cleartext Transmission of Sensitive Information	25-Oct-2023	8.8	The Android Client application, when enrolled with the define method 1 (the user manually inserts the server ip address), use HTTP protocol to retrieve sensitive information (ip address and	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			credentials to connect to a remote MQTT broker entity) instead of HTTPS and this feature is not configurable by the user. Due to the lack of encryption of HTTP,this issue allows an attacker placed in the same subnet network of the HMI device to intercept username and password necessary to authenticate to the MQTT server responsible to implement the remote management protocol. **CVE ID : CVE-2023-45321**		
Missing Authentication for Critical Function	25-Oct-2023	8.8	The Android Client application, when enrolled to the AppHub server,connects to an MQTT broker without enforcing any server authentication. This issue allows an attacker to force the Android Client application to connect to a malicious MQTT broker, enabling it to send fake	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages to the HMI device **CVE ID : CVE-2023-45851**		
Use of Hard-coded Credentials	25-Oct-2023	8.8	The Android Client application, when enrolled to the AppHub server, connects to an MQTT broker to exchange messages and receive commands to execute on the HMI device. The protocol builds on top of MQTT to implement the remote management of the device is encrypted with a hard-coded DES symmetric key, that can be retrieved reversing both the Android Client application and the server-side web application. This issue allows an attacker able to control a malicious MQTT broker on the same subnet network of the device, to craft malicious messages and send them to the HMI device, executing arbitrary	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the device itself. **CVE ID : CVE-2023-46102**		
Use of Hard-coded Credentials	25-Oct-2023	7.8	The vulnerability allows an unprivileged (untrusted) third-party application to arbitrary modify the server settings of the Android Client application, inducing it to connect to an attacker - controlled malicious server.This is possible by forging a valid broadcast intent encrypted with a hardcoded RSA key pair **CVE ID : CVE-2023-41372**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1948
Missing Authorization	25-Oct-2023	7.8	The vulnerability allows a low privileged (untrusted) application to modify a critical system property that should be denied, in order to enable the ADB (Android Debug Bridge) protocol to be exposed on the network, exploiting it to gain a privileged shell on	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the device without requiring the physical access through USB. **CVE ID : CVE-2023-43488**		
N/A	25-Oct-2023	6.8	The vulnerability allows a low privileged user that have access to the device when locked in Kiosk mode to install an arbitrary Android application and leverage it to have access to critical device settings such as the device power management or eventually the device secure settings (ADB debug). **CVE ID : CVE-2023-45844**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1950
N/A	25-Oct-2023	3.3	The vulnerability allows an unprivileged(untrusted) third-party application to interact with a content-provider unsafely exposed by the Android Agent application, potentially modifying sensitive settings of the Android Client application itself.	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	H-BOS-CTRL-281123/1951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-41960		
Vendor: byzoro					
Product: smart_s85f					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-2023	9.8	A vulnerability was found in Beijing Baichuo Smart S85F Management Platform up to 20231010 and classified as critical. This issue affects some unknown processing of the file /sysmanage/importconf.php. The manipulation of the argument btn_file_renew leads to os command 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-243059. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	H-BYZ-SMAR-281123/1952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5683		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-2023	9.8	A vulnerability was found in Beijing Baichuo Smart S85F Management Platform up to 20231012. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /importexport.php. The manipulation leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-243061 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-5684**	N/A	H-BYZ-SMAR-281123/1953
Vendor: Cisco					
Product: catalyst_3650					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature	https://sec.cloudapps.cisco.com	H-CIS-CATA-281123/1954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	
Product: catalyst_3650-12x48fd-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-12x48fd-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Product: catalyst_3650-12x48fd-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1957
Product: catalyst_3650-12x48uq					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-	H-CIS-CATA-281123/1958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	privesc-j22SaA4z	
Product: catalyst_3650-12x48uq-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-12x48uq-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1960
Product: catalyst_3650-12x48uq-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature	https://sec.cloudapps.cisco.com	H-CIS-CATA-281123/1961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	
Product: catalyst_3650-12x48ur					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-12x48ur-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Product: catalyst_3650-12x48ur-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1964
Product: catalyst_3650-12x48ur-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-	H-CIS-CATA-281123/1965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	privesc-j22SaA4z	
Product: catalyst_3650-12x48uz					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-12x48uz-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1967
Product: catalyst_3650-12x48uz-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature	https://sec.cloudapps.cisco.com	H-CIS-CATA-281123/1968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	
Product: catalyst_3650-12x48uz-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-24pd					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Product: catalyst_3650-24pd-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1971
Product: catalyst_3650-24pd-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-	H-CIS-CATA-281123/1972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	privesc-j22SaA4z	
Product: catalyst_3650-24pd-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-24pdm					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1974
Product: catalyst_3650-24pdm-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature	https://sec.cloudapps.cisco.com	H-CIS-CATA-281123/1975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	
Product: catalyst_3650-24pdm-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-24pdm-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Product: catalyst_3650-24ps-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1978
Product: catalyst_3650-24ps-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-	H-CIS-CATA-281123/1979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	privesc-j22SaA4z	
Product: catalyst_3650-24ps-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-24td-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1981
Product: catalyst_3650-24td-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature	https://sec.cloudapps.cisco.com	H-CIS-CATA-281123/1982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	
Product: catalyst_3650-24td-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-24ts-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Product: catalyst_3650-24ts-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1985
Product: catalyst_3650-24ts-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-	H-CIS-CATA-281123/1986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	privesc-j22SaA4z	
Product: catalyst_3650-48fd-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-48fd-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1988
Product: catalyst_3650-48fd-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature	https://sec.cloudapps.cisco.com	H-CIS-CATA-281123/1989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	
Product: catalyst_3650-48fq					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-48fq-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Product: catalyst_3650-48fq-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1992
Product: catalyst_3650-48fq-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-	H-CIS-CATA-281123/1993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	privesc-j22SaA4z	
Product: catalyst_3650-48fqm					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-48fqm-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1995
Product: catalyst_3650-48fqm-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature	https://sec.cloudapps.cisco.com	H-CIS-CATA-281123/1996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	
Product: catalyst_3650-48fqm-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-48fs-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Product: catalyst_3650-48fs-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/1999
Product: catalyst_3650-48fs-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-	H-CIS-CATA-281123/2000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	privesc-j22SaA4z	
Product: catalyst_3650-48pd-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-48pd-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2002
Product: catalyst_3650-48pd-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature	https://sec.cloudapps.cisco.com	H-CIS-CATA-281123/2003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	
Product: catalyst_3650-48pq-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-48pq-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Product: catalyst_3650-48pq-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2006
Product: catalyst_3650-48ps-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-	H-CIS-CATA-281123/2007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	privesc-j22SaA4z	
Product: catalyst_3650-48ps-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-48ps-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2009
Product: catalyst_3650-48td-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature	https://sec.cloudapps.cisco.com	H-CIS-CATA-281123/2010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	
Product: catalyst_3650-48td-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-48td-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Product: catalyst_3650-48tq-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2013
Product: catalyst_3650-48tq-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-	H-CIS-CATA-281123/2014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	privesc-j22SaA4z	
Product: catalyst_3650-48tq-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-48ts-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2016
Product: catalyst_3650-48ts-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature	https://sec.cloudapps.cisco.com	H-CIS-CATA-281123/2017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	
Product: catalyst_3650-48ts-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-8x24pd-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Product: catalyst_3650-8x24pd-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2020
Product: catalyst_3650-8x24pd-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-	H-CIS-CATA-281123/2021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	privesc-j22SaA4z	
Product: catalyst_3650-8x24uq					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3650-8x24uq-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2023
Product: catalyst_3650-8x24uq-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature	https://sec.cloudapps.cisco.com	H-CIS-CATA-281123/2024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	
Product: catalyst_3650-8x24uq-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3850					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Product: catalyst_3850-12s-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2027
Product: catalyst_3850-12s-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-	H-CIS-CATA-281123/2028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	privesc-j22SaA4z	
Product: catalyst_3850-12x48u					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3850-12xs-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2030
Product: catalyst_3850-12xs-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature	https://sec.cloudapps.cisco.com	H-CIS-CATA-281123/2031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	
Product: catalyst_3850-16xs-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3850-16xs-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Product: catalyst_3850-24p-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2034
Product: catalyst_3850-24p-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-	H-CIS-CATA-281123/2035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	privesc-j22SaA4z	
Product: catalyst_3850-24p-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3850-24pw-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2037
Product: catalyst_3850-24s-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature	https://sec.cloudapps.cisco.com	H-CIS-CATA-281123/2038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	
Product: catalyst_3850-24s-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3850-24t-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Product: catalyst_3850-24t-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2041
Product: catalyst_3850-24t-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-	H-CIS-CATA-281123/2042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	privesc-j22SaA4z	
Product: catalyst_3850-24u					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3850-24u-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2044
Product: catalyst_3850-24u-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature	https://sec.cloudapps.cisco.com	H-CIS-CATA-281123/2045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	
Product: catalyst_3850-24u-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3850-24xs					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Product: catalyst_3850-24xs-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2048
Product: catalyst_3850-24xs-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-	H-CIS-CATA-281123/2049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	privesc-j22SaA4z	
Product: catalyst_3850-24xu					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3850-24xu-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2051
Product: catalyst_3850-24xu-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature	https://sec.cloudapps.cisco.com	H-CIS-CATA-281123/2052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	
Product: catalyst_3850-24xu-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3850-32xs-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Product: catalyst_3850-32xs-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2055
Product: catalyst_3850-48f-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-	H-CIS-CATA-281123/2056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	privesc-j22SaA4z	
Product: catalyst_3850-48f-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3850-48f-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2058
Product: catalyst_3850-48p-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature	https://sec.cloudapps.cisco.com	H-CIS-CATA-281123/2059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	
Product: catalyst_3850-48p-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3850-48p-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Product: catalyst_3850-48pw-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2062
Product: catalyst_3850-48t-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-	H-CIS-CATA-281123/2063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	privesc-j22SaA4z	
Product: catalyst_3850-48t-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3850-48t-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2065
Product: catalyst_3850-48u					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature	https://sec.cloudapps.cisco.com	H-CIS-CATA-281123/2066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	
Product: catalyst_3850-48u-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3850-48u-l					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Product: catalyst_3850-48u-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2069
Product: catalyst_3850-48xs					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-	H-CIS-CATA-281123/2070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	privesc-j22SaA4z	
Product: catalyst_3850-48xs-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3850-48xs-f-e					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2072
Product: catalyst_3850-48xs-f-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature	https://sec.cloudapps.cisco.com	H-CIS-CATA-281123/2073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	
Product: catalyst_3850-48xs-s					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Product: catalyst_3850-nm-2-40g					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Product: catalyst_3850-nm-8-10g					
Affected Version(s): -					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	H-CIS-CATA-281123/2076
Vendor: contec					
Product: solarview_compact					
Affected Version(s): -					
N/A	27-Oct-2023	9.8	An issue in Contec SolarView Compact v.6.0 and before allows an attacker to execute arbitrary code via	N/A	H-CON-SOLA-281123/2077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the texteditor.php component. **CVE ID : CVE-2023-46509**		
Vendor: Dlink					
Product: dar-7000					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	9.8	SQL injection vulnerability in D-Link Online behavior audit gateway DAR-7000 V31R02B1413C allows a remote attacker to obtain sensitive information and execute arbitrary code via the editrole.php component. **CVE ID : CVE-2023-42406**	N/A	H-DLI-DAR--281123/2078
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Oct-2023	9.8	D-Link Online behavior audit gateway DAR-7000 V31R02B1413C is vulnerable to SQL Injection via /importexport.php. **CVE ID : CVE-2023-44693**	N/A	H-DLI-DAR--281123/2079
Improper Neutralization of Special Elements used in an SQL Command	17-Oct-2023	9.8	D-Link Online behavior audit gateway DAR-7000 V31R02B1413C is vulnerable to SQL Injection via /log/mailrecvview.php.	N/A	H-DLI-DAR--281123/2080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			**CVE ID : CVE-2023-44694**		
Product: di-7003g					
Affected Version(s): v2.d1					
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the tgfile.htm function. **CVE ID : CVE-2023-45572**	N/A	H-DLI-DI-7-281123/2081
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-	N/A	H-DLI-DI-7-281123/2082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the n parameter of the mrclfile_del.asp function. **CVE ID : CVE-2023-45573**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a	https://www.dlink.com/en/security-bulletin/	H-DLI-DI-7-281123/2083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code via the fn parameter of the file.data function. **CVE ID : CVE-2023-45574**		
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip parameter of the ip_position.asp function. **CVE ID : CVE-2023-45575**	N/A	H-DLI-DI-7-281123/2084
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-	N/A	H-DLI-DI-7-281123/2085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the remove_ext_proto/ remove_ext_port parameter of the upnp_ctrl.asp function. **CVE ID : CVE-2023-45576**		
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-	N/A	H-DLI-DI-7-281123/2086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wanid parameter of the H5/speedlimit.data function. **CVE ID : CVE-2023-45577**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the pap_en/chap_en parameter of the pppoe_base.asp function.	N/A	H-DLI-DI-7-281123/2087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45578		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip/type parameter of the jingx.asp function. **CVE ID : CVE-2023-45579**	N/A	H-DLI-DI-7-281123/2088
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-	N/A	H-DLI-DI-7-281123/2089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wild/mx and other parameters of the ddns.asp function **CVE ID : CVE-2023-45580**		
Product: di-7100g					
Affected Version(s): v2.d1					
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a	N/A	H-DLI-DI-7-281123/2090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code via the fn parameter of the tgfile.htm function. **CVE ID : CVE-2023-45572**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the n parameter of the mrclfile_del.asp function. **CVE ID : CVE-2023-45573**	N/A	H-DLI-DI-7-281123/2091
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-	https://www.dlink.com/en/security-bulletin/	H-DLI-DI-7-281123/2092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the file.data function. **CVE ID : CVE-2023-45574**		
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1	N/A	H-DLI-DI-7-281123/2093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip parameter of the ip_position.asp function. **CVE ID : CVE-2023-45575**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the remove_ext_proto/ remove_ext_port parameter of the upnp_ctrl.asp function. **CVE ID : CVE-2023-45576**	N/A	H-DLI-DI-7-281123/2094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wanid parameter of the H5/speedlimit.data function. **CVE ID : CVE-2023-45577**	N/A	H-DLI-DI-7-281123/2095
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and	N/A	H-DLI-DI-7-281123/2096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the pap_en/chap_en parameter of the pppoe_base.asp function. **CVE ID : CVE-2023-45578**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the	N/A	H-DLI-DI-7-281123/2097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ip/type parameter of the jingx.asp function. **CVE ID : CVE-2023-45579**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wild/mx and other parameters of the ddns.asp function **CVE ID : CVE-2023-45580**	N/A	H-DLI-DI-7-281123/2098
Product: di-7100g\+					
Affected Version(s): v2.d1					
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and	N/A	H-DLI-DI-7-281123/2099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the tgfile.htm function. **CVE ID : CVE-2023-45572**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and	N/A	H-DLI-DI-7-281123/2100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the n parameter of the mrclfile_del.asp function. **CVE ID : CVE-2023-45573**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the file.data function. **CVE ID : CVE-2023-45574**	https://www.dlink.com/en/security-bulletin/	H-DLI-DI-7-281123/2101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip parameter of the ip_position.asp function. **CVE ID : CVE-2023-45575**	N/A	H-DLI-DI-7-281123/2102
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and	N/A	H-DLI-DI-7-281123/2103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the remove_ext_proto/ remove_ext_port parameter of the upnp_ctrl.asp function. **CVE ID : CVE-2023-45576**		
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary	N/A	H-DLI-DI-7-281123/2104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code via the wanid parameter of the H5/speedlimit.data function. **CVE ID : CVE-2023-45577**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the pap_en/chap_en parameter of the pppoe_base.asp function. **CVE ID : CVE-2023-45578**	N/A	H-DLI-DI-7-281123/2105
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-	N/A	H-DLI-DI-7-281123/2106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip/type parameter of the jingx.asp function. **CVE ID : CVE-2023-45579**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and	N/A	H-DLI-DI-7-281123/2107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wild/mx and other parameters of the ddns.asp function **CVE ID : CVE-2023-45580**		
Product: di-7200g					
Affected Version(s): v2.e1					
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the tgfile.htm function. **CVE ID : CVE-2023-45572**	N/A	H-DLI-DI-7-281123/2108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the n parameter of the mrclfile_del.asp function. **CVE ID : CVE-2023-45573**	N/A	H-DLI-DI-7-281123/2109
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and	https://www.dlink.com/en/security-bulletin/	H-DLI-DI-7-281123/2110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the file.data function. **CVE ID : CVE-2023-45574**		
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip parameter of the	N/A	H-DLI-DI-7-281123/2111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ip_position.asp function. **CVE ID : CVE-2023-45575**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the remove_ext_proto/ remove_ext_port parameter of the upnp_ctrl.asp function. **CVE ID : CVE-2023-45576**	N/A	H-DLI-DI-7-281123/2112
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1	N/A	H-DLI-DI-7-281123/2113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wanid parameter of the H5/speedlimit.data function. **CVE ID : CVE-2023-45577**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1	N/A	H-DLI-DI-7-281123/2114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the pap_en/chap_en parameter of the pppoe_base.asp function. **CVE ID : CVE-2023-45578**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip/type parameter of the jingx.asp function. **CVE ID : CVE-2023-45579**	N/A	H-DLI-DI-7-281123/2115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wild/mx and other parameters of the ddns.asp function **CVE ID : CVE-2023-45580**	N/A	H-DLI-DI-7-281123/2116
Product: di-7200g\+					
Affected Version(s): v2.d1					
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-	N/A	H-DLI-DI-7-281123/2117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the tgfile.htm function. **CVE ID : CVE-2023-45572**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the n	N/A	H-DLI-DI-7-281123/2118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter of the mrclfile_del.asp function. **CVE ID : CVE-2023-45573**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the file.data function. **CVE ID : CVE-2023-45574**	https://www.dlink.com/en/security-bulletin/	H-DLI-DI-7-281123/2119
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-	N/A	H-DLI-DI-7-281123/2120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip parameter of the ip_position.asp function. **CVE ID : CVE-2023-45575**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a	N/A	H-DLI-DI-7-281123/2121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code via the remove_ext_proto/ remove_ext_port parameter of the upnp_ctrl.asp function. **CVE ID : CVE-2023-45576**		
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wanid parameter of the H5/speedlimit.data function. **CVE ID : CVE-2023-45577**	N/A	H-DLI-DI-7-281123/2122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the pap_en/chap_en parameter of the pppoe_base.asp function. **CVE ID : CVE-2023-45578**	N/A	H-DLI-DI-7-281123/2123
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1	N/A	H-DLI-DI-7-281123/2124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip/type parameter of the jingx.asp function. **CVE ID : CVE-2023-45579**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the	N/A	H-DLI-DI-7-281123/2125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wild/mx and other parameters of the ddns.asp function **CVE ID : CVE-2023-45580**		
Product: di-7300g\+					
Affected Version(s): v2.d1					
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the tgfile.htm function. **CVE ID : CVE-2023-45572**	N/A	H-DLI-DI-7-281123/2126
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-	N/A	H-DLI-DI-7-281123/2127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the n parameter of the mrclfile_del.asp function. **CVE ID : CVE-2023-45573**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and	https://www.dlink.com/en/security-bulletin/	H-DLI-DI-7-281123/2128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the file.data function. **CVE ID : CVE-2023-45574**		
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip parameter of the ip_position.asp function. **CVE ID : CVE-2023-45575**	N/A	H-DLI-DI-7-281123/2129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the remove_ext_proto/ remove_ext_port parameter of the upnp_ctrl.asp function. **CVE ID : CVE-2023-45576**	N/A	H-DLI-DI-7-281123/2130
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-	N/A	H-DLI-DI-7-281123/2131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wanid parameter of the H5/speedlimit.data function. **CVE ID : CVE-2023-45577**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary	N/A	H-DLI-DI-7-281123/2132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code via the pap_en/chap_en parameter of the pppoe_base.asp function. **CVE ID : CVE-2023-45578**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip/type parameter of the jingx.asp function. **CVE ID : CVE-2023-45579**	N/A	H-DLI-DI-7-281123/2133
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-	N/A	H-DLI-DI-7-281123/2134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wild/mx and other parameters of the ddns.asp function **CVE ID : CVE-2023-45580**		
Product: di-7400g\+					
Affected Version(s): v2.d1					
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-	N/A	H-DLI-DI-7-281123/2135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the tgfile.htm function. **CVE ID : CVE-2023-45572**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the n parameter of the mrclfile_del.asp function. **CVE ID : CVE-2023-45573**	N/A	H-DLI-DI-7-281123/2136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the file.data function. **CVE ID : CVE-2023-45574**	https://www.dlink.com/en/security-bulletin/	H-DLI-DI-7-281123/2137
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-	N/A	H-DLI-DI-7-281123/2138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip parameter of the ip_position.asp function. **CVE ID : CVE-2023-45575**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the remove_ext_proto/ remove_ext_port	N/A	H-DLI-DI-7-281123/2139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter of the upnp_ctrl.asp function. **CVE ID : CVE-2023-45576**		
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wanid parameter of the H5/speedlimit.data function. **CVE ID : CVE-2023-45577**	N/A	H-DLI-DI-7-281123/2140
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and	N/A	H-DLI-DI-7-281123/2141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the pap_en/chap_en parameter of the pppoe_base.asp function. **CVE ID : CVE-2023-45578**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1	N/A	H-DLI-DI-7-281123/2142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip/type parameter of the jingx.asp function. **CVE ID : CVE-2023-45579**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wild/mx and other parameters of the ddns.asp function **CVE ID : CVE-2023-45580**	N/A	H-DLI-DI-7-281123/2143
Product: dir-820l					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Oct-2023	9.8	D-Link DIR-820L 1.05B03 has a stack overflow vulnerability in the sub_4507CC function. **CVE ID : CVE-2023-44808**	N/A	H-DLI-DIR--281123/2144
N/A	16-Oct-2023	9.8	D-Link device DIR-820L 1.05B03 is vulnerable to Insecure Permissions. **CVE ID : CVE-2023-44809**	N/A	H-DLI-DIR--281123/2145
Product: dsl-2730u					
Affected Version(s): -					
N/A	19-Oct-2023	6.8	D-Link (Non-US) DSL-2750U N300 ADSL2+ and (Non-US) DSL-2730U N150 ADSL2+ are vulnerable to Incorrect Access Control. The UART/Serial interface on the PCB, provides log output and a root terminal without proper access control. **CVE ID : CVE-2023-46033**	N/A	H-DLI-DSL--281123/2146
Product: dsl-2750u					
Affected Version(s): -					
N/A	19-Oct-2023	6.8	D-Link (Non-US) DSL-2750U N300 ADSL2+ and (Non-US) DSL-2730U N150 ADSL2+ are	N/A	H-DLI-DSL--281123/2147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to Incorrect Access Control. The UART/Serial interface on the PCB, provides log output and a root terminal without proper access control. **CVE ID : CVE-2023-46033**		
Vendor: Eaton					
Product: easy-box-e4-ac1					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-EASY-281123/2148
Product: easy-box-e4-dc1					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password	https://www.eaton.com/content/dam/eaton/c	H-EAT-EASY-281123/2149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	ompany/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	
Product: easy-box-e4-uc1					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-EASY-281123/2150
Product: easy-e4-ac-12rc1p					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-EASY-281123/2151
Product: easy-e4-ac-12rcx1p					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-EASY-281123/2152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**		
Product: easy-e4-ac-16re1p					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-EASY-281123/2153
Product: easy-e4-dc-12tc1p					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-EASY-281123/2154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**		
Product: easy-e4-dc-12tcx1p					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-EASY-281123/2155
Product: easy-e4-dc-16te1p					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-	H-EAT-EASY-281123/2156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	va-2023-1010.pdf	
Product: easy-e4-dc-4pe1p					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-EASY-281123/2157
Product: easy-e4-dc-6ae1p					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-EASY-281123/2158
Product: easy-e4-dc-8te1p					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending).	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-EASY-281123/2159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43776		
Product: easy-e4-uc-12rc1p					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-EASY-281123/2160
Product: easy-e4-uc-12rcx1p					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-EASY-281123/2161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**		
Product: easy-e4-uc-16re1					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-EASY-281123/2162
Product: easy-e4-uc-16re1p					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-EASY-281123/2163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**		
Product: easy-e4-uc-8re1p					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-EASY-281123/2164
Product: easy_e4-ac-8re1p					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to	https://www.eaton.com/content/dam/eaton/company/news-insights/cybers	H-EAT-EASY-281123/2165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	ecurity/security-bulletins/etn-va-2023-1010.pdf	
Product: xv-102-a035tqrb-1e4					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-XV-1-281123/2166
Product: xv-102-a3-57tvrb-1e4					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-XV-1-281123/2167
Product: xv100-box-e4-dc1					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending).	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-XV10-281123/2168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43776		
Product: xv100-box-e4-uc1					
Affected Version(s): -					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	H-EAT-XV10-281123/2169
Vendor: govee					
Product: led_strip					
Affected Version(s): -					
N/A	30-Oct-2023	7.5	An issue discovered in Govee LED Strip v3.00.42 allows attackers to cause a denial of service via crafted Move and MoveWithOnoff commands. **CVE ID : CVE-2023-45956**	N/A	H-GOV-LED_-281123/2170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: HP					
Product: 200_g4_22_all-in-one_pc_\(rom_family_ssid_86f0\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-200_-281123/2171
Product: 200_g4_22_all-in-one_pc_\(rom_family_ssid_86f2\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-200_-281123/2172
Product: 200_g4_22_all-in-one_pc_\(rom_family_ssid_86f3\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in	https://support.hp.com/us-en/document/i	H-HP-200_-281123/2173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	sh_9461800-9461828-16	
Product: 200_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f0\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-200_-281123/2174
Product: 200_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f2\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-200_-281123/2175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: 200_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f3\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-200_-281123/2176
Product: 205_g4_22_all-in-one_pc_\(rom_family_ssid_86f0\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-205_-281123/2177
Product: 205_g4_22_all-in-one_pc_\(rom_family_ssid_86f2\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-205_-281123/2178
Product: 205_g4_22_all-in-one_pc_\(rom_family_ssid_86f3\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-205_-281123/2179
Product: 205_g8_24_all-in-one_pc_\(rom_family_ssid_8923\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-205_-281123/2180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: 205_g8_24_all-in-one_pc_\(rom_family_ssid_8924\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-205_-281123/2181
Product: 205_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f0\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability.	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-205_-281123/2182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26300		
Product: 205_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f2\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-205_-281123/2183
Product: 205_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f3\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-205_-281123/2184
Product: 205_pro_g8_24_all-in-one_pc_\(rom_family_ssid_8923\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has	https://support.hp.com/us-	H-HP-205_-281123/2185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	en/document/i sh_9461800-9461828-16	
Product: 205_pro_g8_24_all-in-one_pc_\(rom_family_ssid_8924\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-205_-281123/2186
Product: 240_g10					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-240_-281123/2187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: 240_g6					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-240_-281123/2188
Product: 240_g7					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-240_-281123/2189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 240_g9					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-240_-281123/2190
Product: 245					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-245-281123/2191
Product: 245_g10					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC	https://support.hp.com/us-en/document/i	H-HP-245_-281123/2192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	sh_9461800-9461828-16	
Product: 245_g7					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-245_-281123/2193
Product: 245_g8					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-245_-281123/2194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: 245_g9					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-245_-281123/2195
Product: 246_g6					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-246_-281123/2196
Product: 246_g7					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-246_-281123/2197
Product: 247_g8					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-247_-281123/2198
Product: 250_g10					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-250_-281123/2199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: 250_g6					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-250_-281123/2200
Product: 250_g7					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability.	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-250_-281123/2201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26300		
Product: 250_g9					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-250_-281123/2202
Product: 255_g10					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-255_-281123/2203
Product: 255_g6					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has	https://support.hp.com/us-	H-HP-255_-281123/2204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	en/document/ish_9461800-9461828-16	
Product: 255_g7					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-255_-281123/2205
Product: 255_g8					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-255_-281123/2206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: 255_g8_\(rom_family_ssid_87d1\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-255_-281123/2207
Product: 255_g8_\(rom_family_ssid_8905\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-255_-281123/2208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 255_g8_\(rom_family_ssid_890e\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-255_-281123/2209
Product: 255_g9					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-255_-281123/2210
Product: 256_g6					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC	https://support.hp.com/us-en/document/i	H-HP-256_-281123/2211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	sh_9461800-9461828-16	
Product: 256_g7					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-256_-281123/2212
Product: 258_g6					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-258_-281123/2213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: 258_g7					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-258_-281123/2214
Product: 285_g6_microtower_\(rom_family_ssid_871e\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-285_-281123/2215
Product: 285_g8_microtower_\(rom_family_ssid_870e\)					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-285_-281123/2216
Product: 285_pro_g6_microtower_\(rom_family_ssid_871e\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-285_-281123/2217
Product: 285_pro_g8_microtower_\(rom_family_ssid_870e\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-285_-281123/2218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: 295_g8_microtower_\(rom_family_ssid_870e\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-295_-281123/2219
Product: 340_g7					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability.	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-340_-281123/2220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26300		
Product: 348_g7					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-348_-281123/2221
Product: 470_g10					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-470_-281123/2222
Product: 470_g7					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has	https://support.hp.com/us-	H-HP-470_-281123/2223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	en/document/ish_9461800-9461828-16	
Product: 470_g9					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-470_-281123/2224
Product: desktop_pro_a_300_g3					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-DESK-281123/2225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: desktop_pro_a_g3					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-DESK-281123/2226
Product: desktop_pro_a_g3_microtower					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-DESK-281123/2227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: proone_240_g10_\(rom_family_ssid_8b4c\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-PROO-281123/2228
Product: proone_240_g10_\(rom_family_ssid_8b4d\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-PROO-281123/2229
Product: proone_240_g9_\(rom_family_ssid_89eb\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC	https://support.hp.com/us-en/document/i	H-HP-PROO-281123/2230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	sh_9461800-9461828-16	
Product: pro_sff_280_g9_desktop_\(rom_family_ssid_89b4\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-PRO_-281123/2231
Product: pro_sff_280_g9_desktop_\(rom_family_ssid_8bc3\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-PRO_-281123/2232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: pro_sff_290_g9_desktop_\(rom_family_ssid_89b4\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-PRO_-281123/2233
Product: pro_sff_290_g9_desktop_\(rom_family_ssid_8bc3\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-PRO_-281123/2234
Product: pro_sff_zhan_66_g9_desktop_\(rom_family_ssid_89b4\)					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-PRO_-281123/2235
Product: pro_sff_zhan_66_g9_desktop_\(rom_family_ssid_8bc3\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-PRO_-281123/2236
Product: pro_tower_200_g9_desktop_\(rom_family_ssid_89b3\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-PRO_-281123/2237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: pro_tower_200_g9_desktop_\(rom_family_ssid_89b4\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-PRO_-281123/2238
Product: pro_tower_200_g9_desktop_\(rom_family_ssid_8bc3\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability.	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-PRO_-281123/2239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26300		
Product: pro_tower_280_g9_desktop_\(rom_family_ssid_89b3\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-PRO_-281123/2240
Product: pro_tower_280_g9_desktop_\(rom_family_ssid_89b4\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-PRO_-281123/2241
Product: pro_tower_290_g9_desktop_\(rom_family_ssid_89b3\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has	https://support.hp.com/us-	H-HP-PRO_-281123/2242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	en/document/ish_9461800-9461828-16	
Product: pro_tower_290_g9_desktop_\(rom_family_ssid_89b4\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-PRO_-281123/2243
Product: pro_tower_290_g9_desktop_\(rom_family_ssid_8bc3\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-PRO_-281123/2244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: pro_tower_zhan_99_g9_desktop_\(rom_family_ssid_89b3\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-PRO_-281123/2245
Product: pro_tower_zhan_99_g9_desktop_\(rom_family_ssid_89b4\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-PRO_-281123/2246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: pro_tower_zhan_99_g9_desktop_\(rom_family_ssid_8b3c\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-PRO_-281123/2247
Product: stream_11_pro_g4					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-STRE-281123/2248
Product: stream_11_pro_g5					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC	https://support.hp.com/us-en/document/i	H-HP-STRE-281123/2249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	sh_9461800-9461828-16	
Product: t638_thin_client					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-T638-281123/2250
Product: vr_backpack_g2_\(rom_family_ssid_8590\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-VR_B-281123/2251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: zbook_15_g5_mobile_workstation					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-ZBOO-281123/2252
Product: zhan_66_pro_a_g10_\(rom_family_ssid_8b4e\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-ZHAN-281123/2253
Product: zhan_66_pro_a_g1_r_microtower					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-ZHAN-281123/2254
Product: zhan_66_pro_a_g4_all-in-one_pc_\(rom_family_ssid_8923\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-ZHAN-281123/2255
Product: zhan_66_pro_a_g4_all-in-one_pc_\(rom_family_ssid_8924\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-ZHAN-281123/2256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: zhan_99_g3_mobile_workstation					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-ZHAN-281123/2257
Product: zhan_99_g4_mobile_workstation					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability.	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-ZHAN-281123/2258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26300		
Product: zhan_99_pro_a_g2_microtower_\(rom_family_ssid_871e\)					
Affected Version(s): -					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	H-HP-ZHAN-281123/2259
Vendor: hpe					
Product: alletra_4110					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-ALLE-281123/2260
Product: alletra_4120					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service.	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-ALLE-281123/2261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30911		
Product: alletra_4140					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-ALLE-281123/2262
Product: apollo_2000_system					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-APOL-281123/2263
Product: apollo_4200_gen10_plus_system					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-APOL-281123/2264
Product: apollo_4200_gen10_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=	H-HPE-APOL-281123/2265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may cause denial of service. **CVE ID : CVE-2023-30911**	hpesbhf04544en_us	
Product: apollo_4510_gen10_system					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-APOL-281123/2266
Product: apollo_6500_gen10_plus_system					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-APOL-281123/2267
Product: apollo_6500_gen10_system					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-APOL-281123/2268
Product: apollo_n2600_gen10_plus					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and	https://support.hpe.com/hpesc	H-HPE-APOL-281123/2269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	
Product: apollo_n2800_gen10_plus					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-APOL-281123/2270
Product: apollo_r2200_gen10					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-APOL-281123/2271
Product: apollo_r2600_gen10					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-APOL-281123/2272
Product: apollo_r2800_gen10					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-APOL-281123/2273
Product: edgeline_e920d_server_blade					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-EDGE-281123/2274
Product: edgeline_e920t_server_blade					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-EDGE-281123/2275
Product: edgeline_e920_server_blade					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-EDGE-281123/2276
Product: proliant_bl460c_gen10_server_blade					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2277
Product: proliant_dl110_gen10_plus_telco_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2278
Product: proliant_dl110_gen11					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2279
Product: proliant_dl160_gen10_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: proliant_dl180_gen10_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2281
Product: proliant_dl20_gen10_plus_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2282
Product: proliant_dl20_gen10_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2283
Product: proliant_dl20_gen11					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service.	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30911		
Product: proliant_dl320_gen11_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2285
Product: proliant_dl325_gen10_plus_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2286
Product: proliant_dl325_gen10_plus_v2_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2287
Product: proliant_dl325_gen11_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=	H-HPE-PROL-281123/2288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may cause denial of service. **CVE ID : CVE-2023-30911**	hpesbhf04544en_us	
Product: proliant_dl345_gen10_plus_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2289
Product: proliant_dl345_gen11_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2290
Product: proliant_dl360_gen10_plus_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2291
Product: proliant_dl360_gen10_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and	https://support.hpe.com/hpesc	H-HPE-PROL-281123/2292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	
Product: proliant_dl360_gen11_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2293
Product: proliant_dl365_gen10_plus_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2294
Product: proliant_dl365_gen11_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2295
Product: proliant_dl380a_gen11					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2296
Product: proliant_dl380_gen10_plus_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2297
Product: proliant_dl380_gen10_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2298
Product: proliant_dl380_gen11_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2299
Product: proliant_dl385_gen10_plus_server					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2300
Product: proliant_dl385_gen10_plus_v2_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2301
Product: proliant_dl385_gen10_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2302
Product: proliant_dl385_gen11_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: proliant_dl560_gen10_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2304
Product: proliant_dl560_gen11					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2305
Product: proliant_dl580_gen10_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2306
Product: proliant_e910t_server_blade					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service.	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30911		
Product: proliant_e910_server_blade					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2308
Product: proliant_m750_server_blade					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2309
Product: proliant_microserver_gen10_plus					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2310
Product: proliant_microserver_gen10_plus_v2					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=	H-HPE-PROL-281123/2311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may cause denial of service. **CVE ID : CVE-2023-30911**	hpesbhf04544en_us	
Product: proliant_ml110_gen10_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2312
Product: proliant_ml110_gen11					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2313
Product: proliant_ml30_gen10_plus_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2314
Product: proliant_ml30_gen10_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and	https://support.hpe.com/hpesc	H-HPE-PROL-281123/2315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	
Product: proliant_ml30_gen11					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2316
Product: proliant_ml350_gen10_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2317
Product: proliant_ml350_gen11_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2318
Product: proliant_rl300_gen11					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2319
Product: proliant_xl170r_gen10_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2320
Product: proliant_xl190r_gen10_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2321
Product: proliant_xl220n_gen10_plus_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2322
Product: proliant_xl225n_gen10_plus_1u_node					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2323
Product: proliant_xl230k_gen10_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2324
Product: proliant_xl270d_gen10_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2325
Product: proliant_xl290n_gen10_plus_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: proliant_xl2x260w_gen10_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2327
Product: proliant_xl645d_gen10_plus_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2328
Product: proliant_xl675d_gen10_plus_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2329
Product: proliant_xl925g_gen10_plus_1u_4-node_configure-to-order_server					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service.	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-PROL-281123/2330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30911		
Product: synergy_480_gen10_compute_module					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-SYNE-281123/2331
Product: synergy_480_gen10_plus_compute_module					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-SYNE-281123/2332
Product: synergy_480_gen11_compute_module					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	H-HPE-SYNE-281123/2333
Product: synergy_660_gen10_compute_module					
Affected Version(s): -					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=	H-HPE-SYNE-281123/2334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may cause denial of service. **CVE ID : CVE-2023-30911**	hpesbhf04544en_us	
Vendor: Lenovo					
Product: thinkagile_hx1021_edg					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2335
Product: thinkagile_hx1320					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2336
Product: thinkagile_hx1321					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: thinkagile_hx1331					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2338
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2339
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinkagile_hx1520-r					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2341
Product: thinkagile_hx1521-r					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2342
Product: thinkagile_hx2320-e					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: thinkagile_hx2321					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2344
Product: thinkagile_hx2330					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2345
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2347
Product: thinkagile_hx2331					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2348
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2350
Product: thinkagile_hx2720-e					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2351
Product: thinkagile_hx3320					
Affected Version(s): -					
Improper Privilege	25-Oct-2023	8.8	An authenticated XCC user can change	https://support.lenovo.com/us/en/product_se	H-LEN-THIN-281123/2352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Product: thinkagile_hx3321					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2353
Product: thinkagile_hx3330					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2354
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2356
Product: thinkagile_hx3331					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2357
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2359
Product: thinkagile_hx3375					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4607		
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2361
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2362
Product: thinkagile_hx3376					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2363
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2364
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinkagile_hx3520-g					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2366
Product: thinkagile_hx3521-g					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2367
Product: thinkagile_hx3720					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2368
Product: thinkagile_hx3721					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2369
Product: thinkagile_hx5520					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2370
Product: thinkagile_hx5520-c					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2371
Product: thinkagile_hx5521					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted API command. **CVE ID : CVE-2023-4607**		
Product: thinkagile_hx5521-c					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2373
Product: thinkagile_hx5530					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2374
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2376
Product: thinkagile_hx5531					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2377
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2379
Product: thinkagile_hx7520					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4607		
Product: thinkagile_hx7521					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2381
Product: thinkagile_hx7530					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2382
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4606		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2384
Product: thinkagile_hx7531					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2385
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2387
Product: thinkagile_hx7820					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2388
Product: thinkagile_hx7821					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2389
Product: thinkagile_hx_enclosure					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2390
Product: thinkagile_mx1021_on_se350					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2391
Product: thinkagile_mx3330-f_all-flash					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4607		
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2393
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2394
Product: thinkagile_mx3330-h_hybrid					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2395
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2396
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinkagile_mx3331-f_all-flash					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2398
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2399
Improper Neutralization of Special Elements used in an SQL Command	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinkagile_mx3331-h_hybrid					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2401
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4606		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2403
Product: thinkagile_mx3530-h_hybrid					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2404
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2406
Product: thinkagile_mx3530_f_all_flash					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2408
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2409
Product: thinkagile_mx3531-f_all-flash					
Affected Version(s): -					
Improper Privilege	25-Oct-2023	8.8	An authenticated XCC user can change	https://support.lenovo.com/us/en/product_se	H-LEN-THIN-281123/2410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2411
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4608		
Product: thinkagile_mx3531_h_hybrid					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2413
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2414
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinkagile_mx630_v3_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2416
Product: thinkagile_mx630_v3_intergrated_system_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2417
Product: thinkagile_mx650_v3_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4607		
Product: thinkagile_mx650_v3_intergrated_system_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2419
Product: thinkagile_mx_edge-_mx1020_					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2420
Product: thinkagile_vx1320					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2421
Product: thinkagile_vx2320					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2422
Product: thinkagile_vx2330					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2423
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2424
Improper Neutralization of	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges	https://support.lenovo.com/us/en/product_se	H-LEN-THIN-281123/2425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	curity/LEN-140960	
Product: thinkagile_vx3320					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2426
Product: thinkagile_vx3330					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2427
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only	https://support.lenovo.com/us/en/product_se	H-LEN-THIN-281123/2428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	curity/LEN-140960	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2429
Product: thinkagile_vx3331					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted API command. **CVE ID : CVE-2023-4607**		
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2431
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: thinkagile_vx3520-g					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2433
Product: thinkagile_vx3530-g					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2434
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2436
Product: thinkagile_vx3720					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2437
Product: thinkagile_vx5520					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: thinkagile_vx5530					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2439
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2440
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinkagile_vx7320_n					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2442
Product: thinkagile_vx7330					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2443
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2445
Product: thinkagile_vx7520					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2446
Product: thinkagile_vx7520_n					
Affected Version(s): -					
Improper Privilege	25-Oct-2023	8.8	An authenticated XCC user can change	https://support.lenovo.com/us/en/product_se	H-LEN-THIN-281123/2447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Product: thinkagile_vx7530					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2448
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2449
Improper Neutralization of Special Elements used in an	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinkagile_vx7531					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2451
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4606		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2453
Product: thinkagile_vx7820					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2454
Product: thinkagile_vx_1se					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4607		
Product: thinkagile_vx_2u4n					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2456
Product: thinkagile_vx_4u					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2457
Product: thinkedge_se450					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2458
Product: thinkpad_t14_gen_3					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	25-Oct-2023	7.8	A vulnerability was reported in Elliptic Labs Virtual Lock Sensor for ThinkPad T14 Gen 3 that could allow an attacker with local access to execute code with elevated privileges. **CVE ID : CVE-2023-3112**	https://support.lenovo.com/us/en/product_security/LEN-128081	H-LEN-THIN-281123/2459
Product: thinkserver_sr590					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2460
Product: thinksystem_sd530					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2461
Product: thinksystem_sd630_v2					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for	https://support.lenovo.com/us/en/product_se	H-LEN-THIN-281123/2462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			any user through a crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2463
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: thinksystem_sd650-n_v2					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2465
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2466
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinksystem_sd650_dual_node_tray					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2468
Product: thinksystem_sd650_dwc_dual_node_tray					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2469
Product: thinksystem_sd650_v2					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2471
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2472
Product: thinksystem_se350					
Affected Version(s): -					
Improper Privilege	25-Oct-2023	8.8	An authenticated XCC user can change	https://support.lenovo.com/us/en/product_se	H-LEN-THIN-281123/2473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Product: thinksystem_sn550					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2474
Product: thinksystem_sn550_v2					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2475
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2477
Product: thinksystem_sn850					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2478
Product: thinksystem_sr150					
Affected Version(s): -					
Improper Privilege	25-Oct-2023	8.8	An authenticated XCC user can change	https://support.lenovo.com/us/en/product_se	H-LEN-THIN-281123/2479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Product: thinksystem_sr158					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2480
Product: thinksystem_sr250					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2481
Product: thinksystem_sr250_v2					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2483
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2484
Product: thinksystem_sr258					
Affected Version(s): -					
Improper Privilege	25-Oct-2023	8.8	An authenticated XCC user can change	https://support.lenovo.com/us/en/product_se	H-LEN-THIN-281123/2485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Product: thinksystem_sr258_v2					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2486
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2487
Improper Neutralization of Special Elements used in an	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinksystem_sr530					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2489
Product: thinksystem_sr550					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2490
Product: thinksystem_sr570					
Affected Version(s): -					
Improper Privilege	25-Oct-2023	8.8	An authenticated XCC user can change	https://support.lenovo.com/us/en/product_se	H-LEN-THIN-281123/2491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Product: thinksystem_sr630					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2492
Product: thinksystem_sr630_v2					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2493
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2495
Product: thinksystem_sr645					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2496
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2498
Product: thinksystem_sr645_v3					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4607		
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2500
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2501
Product: thinksystem_sr650					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2502
Product: thinksystem_sr650_v2					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2503
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2504
Improper Neutralization of	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges	https://support.lenovo.com/us/en/product_se	H-LEN-THIN-281123/2505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	curity/LEN-140960	
Product: thinksystem_sr665					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2506
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2508
Product: thinksystem_sr670					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2509
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2511
Product: thinksystem_sr670_v2					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4607		
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2513
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2514
Product: thinksystem_sr850					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2515
Product: thinksystem_sr850p					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2516
Product: thinksystem_sr850_v2					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2517
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2519
Product: thinksystem_sr860					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2520
Product: thinksystem_sr860_v2					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2521
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2522
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinksystem_sr950					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2524
Product: thinksystem_st250					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2525
Product: thinksystem_st250_v2					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2527
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2528
Product: thinksystem_st258					
Affected Version(s): -					
Improper Privilege	25-Oct-2023	8.8	An authenticated XCC user can change	https://support.lenovo.com/us/en/product_se	H-LEN-THIN-281123/2529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Product: thinksystem_st258_v2					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2530
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2531
Improper Neutralization of Special Elements used in an	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinksystem_st550					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2533
Product: thinksystem_st650_v2					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2534
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2536
Product: thinksystem_st658_v2					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4607		
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2538
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	H-LEN-THIN-281123/2539
Vendor: Mercurycom					
Product: a15					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	25-Oct-2023	9.8	Mercury A15 V1.0 20230818_1.0.3 was discovered to contain a command execution vulnerability via the component cloudDeviceToken SuccCB. **CVE ID : CVE-2023-46518**	N/A	H-MER-A15-281123/2540
Vendor: nanoleaf					
Product: lightstrip					
Affected Version(s): -					
N/A	31-Oct-2023	7.5	An issue discovered in Nanoleaf Light strip v3.5.10 allows attackers to cause a denial of service via crafted write binding attribute commands. **CVE ID : CVE-2023-45955**	N/A	H-NAN-LIGH-281123/2541
Vendor: netmodule					
Product: nb1601					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Oct-2023	6.6	The web administration interface in NetModule Router Software (NRSW) 4.6 before 4.6.0.106 and 4.8 before 4.8.0.101 executes an OS command constructed with	N/A	H-NET-NB16-281123/2542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unsanitized user input: shell metacharacters in the /admin/gnssAutoAlign.php device_id parameter. This occurs because another thread can be started before the trap that triggers the cleanup function. A successful exploit could allow an authenticated user to execute arbitrary commands with elevated privileges. NOTE: this is different from CVE-2023-0861 and CVE-2023-0862, which were fixed in version 4.6.0.105. **CVE ID : CVE-2023-46306**		
Product: nb1800					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Oct-2023	6.6	The web administration interface in NetModule Router Software (NRSW) 4.6 before 4.6.0.106 and 4.8 before 4.8.0.101 executes an OS command constructed with unsanitized user input: shell	N/A	H-NET-NB18-281123/2543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			metacharacters in the /admin/gnssAutoAlign.php device_id parameter. This occurs because another thread can be started before the trap that triggers the cleanup function. A successful exploit could allow an authenticated user to execute arbitrary commands with elevated privileges. NOTE: this is different from CVE-2023-0861 and CVE-2023-0862, which were fixed in version 4.6.0.105. **CVE ID : CVE-2023-46306**		
Product: nb1810					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Oct-2023	6.6	The web administration interface in NetModule Router Software (NRSW) 4.6 before 4.6.0.106 and 4.8 before 4.8.0.101 executes an OS command constructed with unsanitized user input: shell metacharacters in the	N/A	H-NET-NB18-281123/2544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/admin/gnssAutoAlign.php device_id parameter. This occurs because another thread can be started before the trap that triggers the cleanup function. A successful exploit could allow an authenticated user to execute arbitrary commands with elevated privileges. NOTE: this is different from CVE-2023-0861 and CVE-2023-0862, which were fixed in version 4.6.0.105. **CVE ID : CVE-2023-46306**		
Product: nb2800					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Oct-2023	6.6	The web administration interface in NetModule Router Software (NRSW) 4.6 before 4.6.0.106 and 4.8 before 4.8.0.101 executes an OS command constructed with unsanitized user input: shell metacharacters in the /admin/gnssAutoAlign.php device_id	N/A	H-NET-NB28-281123/2545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter. This occurs because another thread can be started before the trap that triggers the cleanup function. A successful exploit could allow an authenticated user to execute arbitrary commands with elevated privileges. NOTE: this is different from CVE-2023-0861 and CVE-2023-0862, which were fixed in version 4.6.0.105. **CVE ID : CVE-2023-46306**		
Product: nb2810					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Oct-2023	6.6	The web administration interface in NetModule Router Software (NRSW) 4.6 before 4.6.0.106 and 4.8 before 4.8.0.101 executes an OS command constructed with unsanitized user input: shell metacharacters in the /admin/gnssAutoAlign.php device_id parameter. This occurs because	N/A	H-NET-NB28-281123/2546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			another thread can be started before the trap that triggers the cleanup function. A successful exploit could allow an authenticated user to execute arbitrary commands with elevated privileges. NOTE: this is different from CVE-2023-0861 and CVE-2023-0862, which were fixed in version 4.6.0.105. **CVE ID : CVE-2023-46306**		
Product: nb3701					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Oct-2023	6.6	The web administration interface in NetModule Router Software (NRSW) 4.6 before 4.6.0.106 and 4.8 before 4.8.0.101 executes an OS command constructed with unsanitized user input: shell metacharacters in the /admin/gnssAutoAlign.php device_id parameter. This occurs because another thread can be started before	N/A	H-NET-NB37-281123/2547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the trap that triggers the cleanup function. A successful exploit could allow an authenticated user to execute arbitrary commands with elevated privileges. NOTE: this is different from CVE-2023-0861 and CVE-2023-0862, which were fixed in version 4.6.0.105. **CVE ID : CVE-2023-46306**		
Product: nb3800					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Oct-2023	6.6	The web administration interface in NetModule Router Software (NRSW) 4.6 before 4.6.0.106 and 4.8 before 4.8.0.101 executes an OS command constructed with unsanitized user input: shell metacharacters in the /admin/gnssAutoAlign.php device_id parameter. This occurs because another thread can be started before the trap that triggers the	N/A	H-NET-NB38-281123/2548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cleanup function. A successful exploit could allow an authenticated user to execute arbitrary commands with elevated privileges. NOTE: this is different from CVE-2023-0861 and CVE-2023-0862, which were fixed in version 4.6.0.105. **CVE ID : CVE-2023-46306**		
Product: ng800					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Oct-2023	6.6	The web administration interface in NetModule Router Software (NRSW) 4.6 before 4.6.0.106 and 4.8 before 4.8.0.101 executes an OS command constructed with unsanitized user input: shell metacharacters in the /admin/gnssAutoAlign.php device_id parameter. This occurs because another thread can be started before the trap that triggers the cleanup function. A successful exploit	N/A	H-NET-NG80-281123/2549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated user to execute arbitrary commands with elevated privileges. NOTE: this is different from CVE-2023-0861 and CVE-2023-0862, which were fixed in version 4.6.0.105. **CVE ID : CVE-2023-46306**		
Vendor: nxp					
Product: i.mx_8m					
Affected Version(s): -					
Improper Preservation of Permissions	17-Oct-2023	7.8	A software vulnerability has been identified in the U-Boot Secondary Program Loader (SPL) before 2023.07 on select NXP i.MX 8M family processors. Under certain conditions, a crafted Flattened Image Tree (FIT) format structure can be used to overwrite SPL memory, allowing unauthenticated software to execute on the target, leading to privilege escalation. This affects i.MX 8M, i.MX 8M Mini, i.MX	https://community.nxp.com/t5/i-MX-Security/U-Boot-Secondary-Program-Loader-Authentication-Vulnerability-CVE/ta-p/1736196	H-NXP-I.MX-281123/2550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8M Nano, and i.MX 8M Plus. **CVE ID : CVE-2023-39902**		
Product: i.mx_8m_mini					
Affected Version(s): -					
Improper Preservation of Permissions	17-Oct-2023	7.8	A software vulnerability has been identified in the U-Boot Secondary Program Loader (SPL) before 2023.07 on select NXP i.MX 8M family processors. Under certain conditions, a crafted Flattened Image Tree (FIT) format structure can be used to overwrite SPL memory, allowing unauthenticated software to execute on the target, leading to privilege escalation. This affects i.MX 8M, i.MX 8M Mini, i.MX 8M Nano, and i.MX 8M Plus. **CVE ID : CVE-2023-39902**	https://community.nxp.com/t5/i-MX-Security/U-Boot-Secondary-Program-Loader-Authentication-Vulnerability-CVE/ta-p/1736196	H-NXP-I.MX-281123/2551
Product: i.mx_8m_nano					
Affected Version(s): -					
Improper Preservation of	17-Oct-2023	7.8	A software vulnerability has been identified in the U-Boot	https://community.nxp.com/t5/i-MX-Security/U-	H-NXP-I.MX-281123/2552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permissions			Secondary Program Loader (SPL) before 2023.07 on select NXP i.MX 8M family processors. Under certain conditions, a crafted Flattened Image Tree (FIT) format structure can be used to overwrite SPL memory, allowing unauthenticated software to execute on the target, leading to privilege escalation. This affects i.MX 8M, i.MX 8M Mini, i.MX 8M Nano, and i.MX 8M Plus. **CVE ID : CVE-2023-39902**	Boot-Secondary-Program-Loader-Authentication-Vulnerability-CVE/ta-p/1736196	
Product: i.mx_8m_plus					
Affected Version(s): -					
Improper Preservation of Permissions	17-Oct-2023	7.8	A software vulnerability has been identified in the U-Boot Secondary Program Loader (SPL) before 2023.07 on select NXP i.MX 8M family processors. Under certain conditions, a crafted Flattened Image Tree (FIT) format structure can be used to	https://community.nxp.com/t5/i-MX-Security/U-Boot-Secondary-Program-Loader-Authentication-Vulnerability-CVE/ta-p/1736196	H-NXP-I.MX-281123/2553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overwrite SPL memory, allowing unauthenticated software to execute on the target, leading to privilege escalation. This affects i.MX 8M, i.MX 8M Mini, i.MX 8M Nano, and i.MX 8M Plus. **CVE ID : CVE-2023-39902**		
Vendor: sick					
Product: fx0-gent00000					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	H-SIC-FX0--281123/2554
Product: fx0-gent00010					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	H-SIC-FX0--281123/2555
Product: fx0-gent00030					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	H-SIC-FX0--281123/2556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**		
Product: fx0-gepr00000					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	H-SIC-FX0--281123/2557
Product: fx0-gepr00010					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with	https://sick.com/.well-known/csaf/white/2023/sca-	H-SIC-FX0--281123/2558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	
Product: fx0-get00000					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	H-SIC-FX0--281123/2559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass by capture-replay. **CVE ID : CVE-2023-5246**		
Product: fx0-get00010					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	H-SIC-FX0--281123/2560
Product: fx0-gmod00000					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487,	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-	H-SIC-FX0--281123/2561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	known/csaf/white/2023/sca-2023-0011.json	
Product: fx0-gmod00010					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	H-SIC-FX0--281123/2562
Product: fx0-gmod00030					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	H-SIC-FX0--281123/2563
Product: fx0-gpnt00000					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	H-SIC-FX0--281123/2564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**		
Product: fx0-gpnt00010					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	H-SIC-FX0--281123/2565
Product: fx0-gpnt00030					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with	https://sick.com/.well-known/csaf/white/2023/sca-	H-SIC-FX0--281123/2566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	
Vendor: sielco					
Product: analog_fm_transmitter_exc1000gt					
Affected Version(s): 1.6.3					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	H-SIE-ANAL-281123/2567
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A	N/A	H-SIE-ANAL-281123/2568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**		
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	H-SIE-ANAL-281123/2569
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and	N/A	H-SIE-ANAL-281123/2570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**		
Product: analog_fm_transmitter_exc1000gx					
Affected Version(s): 2.08					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	H-SIE-ANAL-281123/2571
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	H-SIE-ANAL-281123/2572
Cross-Site Request	26-Oct-2023	8.8	The application interface allows	N/A	H-SIE-ANAL-281123/2573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**		
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	H-SIE-ANAL-281123/2574
Product: analog_fm_transmitter_exc100gt					
Affected Version(s): 1.7.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	H-SIE-ANAL-281123/2575
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	H-SIE-ANAL-281123/2576
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to	N/A	H-SIE-ANAL-281123/2577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**		
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	H-SIE-ANAL-281123/2578
Product: analog_fm_transmitter_exc120gt					
Affected Version(s): 1.5.4					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and	N/A	H-SIE-ANAL-281123/2579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulate the transmitter. **CVE ID : CVE-2023-42769**		
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	H-SIE-ANAL-281123/2580
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	H-SIE-ANAL-281123/2581
N/A	26-Oct-2023	6.5	The application suffers from improper access	N/A	H-SIE-ANAL-281123/2582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**		
Product: analog_fm_transmitter_exc120gx					
Affected Version(s): 2.12					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	H-SIE-ANAL-281123/2583
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST	N/A	H-SIE-ANAL-281123/2584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to set a parameter. **CVE ID : CVE-2023-41966**		
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	H-SIE-ANAL-281123/2585
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters.	N/A	H-SIE-ANAL-281123/2586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45228		
Product: analog_fm_transmitter_exc1600gx					
Affected Version(s): 2.08					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	H-SIE-ANAL-281123/2587
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	H-SIE-ANAL-281123/2588
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any	N/A	H-SIE-ANAL-281123/2589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**		
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	H-SIE-ANAL-281123/2590
Affected Version(s): 2.10					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid	N/A	H-SIE-ANAL-281123/2591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**		
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	H-SIE-ANAL-281123/2592
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	H-SIE-ANAL-281123/2593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	H-SIE-ANAL-281123/2594
Product: analog_fm_transmitter_exc2000gx					
Affected Version(s): 2.10					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	H-SIE-ANAL-281123/2595
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can	N/A	H-SIE-ANAL-281123/2596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**		
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	H-SIE-ANAL-281123/2597
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST	N/A	H-SIE-ANAL-281123/2598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request with modified parameters. **CVE ID : CVE-2023-45228**		
Product: analog_fm_transmitter_exc3000gx					
Affected Version(s): 2.07					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	H-SIE-ANAL-281123/2599
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	H-SIE-ANAL-281123/2600
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via	N/A	H-SIE-ANAL-281123/2601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**		
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	H-SIE-ANAL-281123/2602
Product: analog_fm_transmitter_exc300gt					
Affected Version(s): 1.7.4					
Improper Restriction of Excessive	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by	N/A	H-SIE-ANAL-281123/2603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Attempts			brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**		
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	H-SIE-ANAL-281123/2604
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user	N/A	H-SIE-ANAL-281123/2605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			visits a malicious web site. **CVE ID : CVE-2023-45317**		
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	H-SIE-ANAL-281123/2606
Product: analog_fm_transmitter_exc300gx					
Affected Version(s): 2.11					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	H-SIE-ANAL-281123/2607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	H-SIE-ANAL-281123/2608
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	H-SIE-ANAL-281123/2609
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can	N/A	H-SIE-ANAL-281123/2610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**		
Product: analog_fm_transmitter_exc30gt					
Affected Version(s): 1.7.7					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	H-SIE-ANAL-281123/2611
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	H-SIE-ANAL-281123/2612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	H-SIE-ANAL-281123/2613
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	H-SIE-ANAL-281123/2614
Product: analog_fm_transmitter_exc5000gt					
Affected Version(s): 1.7.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	H-SIE-ANAL-281123/2615
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	H-SIE-ANAL-281123/2616
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with	N/A	H-SIE-ANAL-281123/2617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**		
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	H-SIE-ANAL-281123/2618
Product: analog_fm_transmitter_exc5000gx					
Affected Version(s): 2.12					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter.	N/A	H-SIE-ANAL-281123/2619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-42769		
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	H-SIE-ANAL-281123/2620
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	H-SIE-ANAL-281123/2621
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users.	N/A	H-SIE-ANAL-281123/2622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**		
Affected Version(s): 2.06					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	H-SIE-ANAL-281123/2623
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	H-SIE-ANAL-281123/2624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	H-SIE-ANAL-281123/2625
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	H-SIE-ANAL-281123/2626
Product: polyeco1000					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Session Fixation	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to a session hijack vulnerability due to the cookie being vulnerable to a brute force attack, lack of SSL, and the session being visible in requests. **CVE ID : CVE-2023-0897**	N/A	H-SIE-POLY-281123/2627
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an attacker escalating their privileges by modifying passwords in POST requests. **CVE ID : CVE-2023-46661**	N/A	H-SIE-POLY-281123/2628
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an authentication bypass vulnerability due to an attacker modifying passwords in a POST request and gain unauthorized access to the affected device with administrative privileges. **CVE ID : CVE-2023-46665**	N/A	H-SIE-POLY-281123/2629
Improper Restriction of Excessive	26-Oct-2023	9.8	Sielco PolyEco1000 uses a weak set of default administrative	N/A	H-SIE-POLY-281123/2630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Attempts			credentials that can be easily guessed in remote password attacks and gain full control of the system. **CVE ID : CVE-2023-5754**		
N/A	26-Oct-2023	9.1	Sielco PolyEco1000 is vulnerable to an improper access control vulnerability when the application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources behind protected pages. **CVE ID : CVE-2023-46664**	N/A	H-SIE-POLY-281123/2631
N/A	26-Oct-2023	8.1	Sielco PolyEco1000 is vulnerable to an attacker bypassing authorization and accessing resources behind protected pages. The application interface allows users to perform certain actions via HTTP requests without performing any	N/A	H-SIE-POLY-281123/2632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validity checks to verify the requests. **CVE ID : CVE-2023-46663**		
N/A	26-Oct-2023	7.5	Sielco PolyEco1000 is vulnerable to an information disclosure vulnerability due to improper access control enforcement. An unauthenticated remote attacker can exploit this via a specially crafted request to gain access to sensitive information. **CVE ID : CVE-2023-46662**	N/A	H-SIE-POLY-281123/2633
Product: polyeco300					
Affected Version(s): -					
Session Fixation	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to a session hijack vulnerability due to the cookie being vulnerable to a brute force attack, lack of SSL, and the session being visible in requests. **CVE ID : CVE-2023-0897**	N/A	H-SIE-POLY-281123/2634
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an attacker escalating their privileges by modifying	N/A	H-SIE-POLY-281123/2635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passwords in POST requests. **CVE ID : CVE-2023-46661**		
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an authentication bypass vulnerability due to an attacker modifying passwords in a POST request and gain unauthorized access to the affected device with administrative privileges. **CVE ID : CVE-2023-46665**	N/A	H-SIE-POLY-281123/2636
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	Sielco PolyEco1000 uses a weak set of default administrative credentials that can be easily guessed in remote password attacks and gain full control of the system. **CVE ID : CVE-2023-5754**	N/A	H-SIE-POLY-281123/2637
N/A	26-Oct-2023	9.1	Sielco PolyEco1000 is vulnerable to an improper access control vulnerability when the application provides direct access to objects	N/A	H-SIE-POLY-281123/2638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources behind protected pages. **CVE ID : CVE-2023-46664**		
N/A	26-Oct-2023	8.1	Sielco PolyEco1000 is vulnerable to an attacker bypassing authorization and accessing resources behind protected pages. The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. **CVE ID : CVE-2023-46663**	N/A	H-SIE-POLY-281123/2639
N/A	26-Oct-2023	7.5	Sielco PolyEco1000 is vulnerable to an information disclosure vulnerability due to improper access control enforcement. An unauthenticated remote attacker can exploit this via a specially crafted request to gain	N/A	H-SIE-POLY-281123/2640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to sensitive information. **CVE ID : CVE-2023-46662**		
Product: polyeco500					
Affected Version(s): -					
Session Fixation	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to a session hijack vulnerability due to the cookie being vulnerable to a brute force attack, lack of SSL, and the session being visible in requests. **CVE ID : CVE-2023-0897**	N/A	H-SIE-POLY-281123/2641
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an attacker escalating their privileges by modifying passwords in POST requests. **CVE ID : CVE-2023-46661**	N/A	H-SIE-POLY-281123/2642
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an authentication bypass vulnerability due to an attacker modifying passwords in a POST request and gain unauthorized access to the affected device with	N/A	H-SIE-POLY-281123/2643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrative privileges. **CVE ID : CVE-2023-46665**		
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	Sielco PolyEco1000 uses a weak set of default administrative credentials that can be easily guessed in remote password attacks and gain full control of the system. **CVE ID : CVE-2023-5754**	N/A	H-SIE-POLY-281123/2644
N/A	26-Oct-2023	9.1	Sielco PolyEco1000 is vulnerable to an improper access control vulnerability when the application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources behind protected pages. **CVE ID : CVE-2023-46664**	N/A	H-SIE-POLY-281123/2645
N/A	26-Oct-2023	8.1	Sielco PolyEco1000 is vulnerable to an attacker bypassing authorization and accessing	N/A	H-SIE-POLY-281123/2646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resources behind protected pages. The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. **CVE ID : CVE-2023-46663**		
N/A	26-Oct-2023	7.5	Sielco PolyEco1000 is vulnerable to an information disclosure vulnerability due to improper access control enforcement. An unauthenticated remote attacker can exploit this via a specially crafted request to gain access to sensitive information. **CVE ID : CVE-2023-46662**	N/A	H-SIE-POLY-281123/2647
Product: radio_link_exc19					
Affected Version(s): 1.55					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid	N/A	H-SIE-RADI-281123/2648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**		
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	H-SIE-RADI-281123/2649
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	H-SIE-RADI-281123/2650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	H-SIE-RADI-281123/2651
Affected Version(s): 2.00					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	H-SIE-RADI-281123/2652
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges	N/A	H-SIE-RADI-281123/2653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**		
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	H-SIE-RADI-281123/2654
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified	N/A	H-SIE-RADI-281123/2655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameters. **CVE ID : CVE-2023-45228**		
Product: radio_link_rtx19					
Affected Version(s): 2.06					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	H-SIE-RADI-281123/2656
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	H-SIE-RADI-281123/2657
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any	N/A	H-SIE-RADI-281123/2658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**		
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	H-SIE-RADI-281123/2659
Affected Version(s): 1.59					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid	N/A	H-SIE-RADI-281123/2660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**		
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	H-SIE-RADI-281123/2661
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	H-SIE-RADI-281123/2662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	H-SIE-RADI-281123/2663
Affected Version(s): 1.60					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	H-SIE-RADI-281123/2664
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges	N/A	H-SIE-RADI-281123/2665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**		
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	H-SIE-RADI-281123/2666
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST	N/A	H-SIE-RADI-281123/2667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request with modified parameters. **CVE ID : CVE-2023-45228**		
Affected Version(s): 2.05					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	H-SIE-RADI-281123/2668
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	H-SIE-RADI-281123/2669
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any	N/A	H-SIE-RADI-281123/2670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**		
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	H-SIE-RADI-281123/2671
Vendor: Sonicwall					
Product: nsa2700					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA2-281123/2672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**		
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA2-281123/2673
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA2-281123/2674
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA2-281123/2675
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure	https://psirt.global.sonicwall.com/vuln-	H-SON-NSA2-281123/2676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	detail/SNWLID-2023-0012	
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA2-281123/2677
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA2-281123/2678
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA2-281123/2679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA2-281123/2680
Product: nsa3700					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA3-281123/2681
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA3-281123/2682
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.js	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA3-281123/2683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA3-281123/2684
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA3-281123/2685
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA3-281123/2686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA3-281123/2687
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA3-281123/2688
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA3-281123/2689
Product: nsa4700					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA4-281123/2690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**		
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA4-281123/2691
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA4-281123/2692
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA4-281123/2693
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure	https://psirt.global.sonicwall.com/vuln-	H-SON-NSA4-281123/2694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	detail/SNWLID-2023-0012	
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA4-281123/2695
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA4-281123/2696
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA4-281123/2697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA4-281123/2698
Product: nsa5700					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA5-281123/2699
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA5-281123/2700
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA5-281123/2701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to a firewall crash. **CVE ID : CVE-2023-39276**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA5-281123/2702
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA5-281123/2703
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA5-281123/2704
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer	https://psirt.global.sonicwall.com/vuln-	H-SON-NSA5-281123/2705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	detail/SNWLID-2023-0012	
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA5-281123/2706
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA5-281123/2707
Product: nsa6700					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA6-281123/2708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			their privileges inside the tunnel. **CVE ID : CVE-2023-41715**		
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA6-281123/2709
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA6-281123/2710
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA6-281123/2711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA6-281123/2712
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA6-281123/2713
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA6-281123/2714
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA6-281123/2715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA6-281123/2716
Product: nsa_2600					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2717
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2719
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2720
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2721
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2723
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2724
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2725
Product: nsa_2650					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2726
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2727
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2728
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to a firewall crash. **CVE ID : CVE-2023-39277**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2730
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2731
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2732
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow	https://psirt.global.sonicwall.com/vuln-	H-SON-NSA_-281123/2733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	detail/SNWLID-2023-0012	
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2734
Product: nsa_3600					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2735
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2737
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2738
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2739
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2741
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2742
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2743
Product: nsa_3650					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2744
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2745
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2746
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to a firewall crash. **CVE ID : CVE-2023-39277**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2748
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2749
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2750
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow	https://psirt.global.sonicwall.com/vuln-	H-SON-NSA_-281123/2751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	detail/SNWLID-2023-0012	
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2752
Product: nsa_4600					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2753
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2755
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2756
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2757
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2759
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2760
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2761
Product: nsa_4650					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2762
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2763
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2764
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to a firewall crash. **CVE ID : CVE-2023-39277**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2766
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2767
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2768
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow	https://psirt.global.sonicwall.com/vuln-	H-SON-NSA_-281123/2769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	detail/SNWLID-2023-0012	
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2770
Product: nsa_5600					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2771
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2773
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2774
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2775
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2777
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2778
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2779
Product: nsa_5650					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2780
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2781
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2782
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2784
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2785
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2786
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2788
Product: nsa_6600					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2789
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2791
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2792
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2793
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2795
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2796
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2797
Product: nsa_6650					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2798
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2799
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2800
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2802
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2803
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2804
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSA_-281123/2806
Product: nssp10700					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2807
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2809
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2810
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2811
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2813
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2814
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2815
Product: nssp11700					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2816
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2817
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2818
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2820
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2821
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2822
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2824
Product: nssp13700					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2825
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2827
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2828
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2829
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2831
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2832
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2833
Product: nssp15700					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2834
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2835
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2836
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2838
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2839
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2840
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSSP-281123/2842
Product: nsv10					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2843
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2845
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2846
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2847
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2849
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2850
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2851
Product: nsv100					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2852
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2853
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2854
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2856
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2857
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2858
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2860
Product: nsv1600					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2861
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2863
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2864
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2865
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2867
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2868
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV1-281123/2869
Product: nsv200					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2870
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2871
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2872
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2874
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2875
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2876
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2878
Product: nsv25					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2879
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2881
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2882
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2883
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2885
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2886
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2887
Product: nsv270					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2888
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2889
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2890
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2892
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2893
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2894
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV2-281123/2896
Product: nsv300					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV3-281123/2897
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV3-281123/2898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV3-281123/2899
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV3-281123/2900
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV3-281123/2901
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV3-281123/2902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV3-281123/2903
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV3-281123/2904
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV3-281123/2905
Product: nsv400					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV4-281123/2906
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV4-281123/2907
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV4-281123/2908
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV4-281123/2909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV4-281123/2910
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV4-281123/2911
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV4-281123/2912
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV4-281123/2913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV4-281123/2914
Product: nsv470					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV4-281123/2915
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV4-281123/2916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV4-281123/2917
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV4-281123/2918
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV4-281123/2919
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV4-281123/2920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV4-281123/2921
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV4-281123/2922
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV4-281123/2923
Product: nsv50					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV5-281123/2924
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV5-281123/2925
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV5-281123/2926
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV5-281123/2927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV5-281123/2928
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV5-281123/2929
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV5-281123/2930
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV5-281123/2931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV5-281123/2932
Product: nsv800					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV8-281123/2933
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV8-281123/2934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV8-281123/2935
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV8-281123/2936
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV8-281123/2937
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV8-281123/2938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV8-281123/2939
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV8-281123/2940
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV8-281123/2941
Product: nsv870					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV8-281123/2942
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV8-281123/2943
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV8-281123/2944
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV8-281123/2945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV8-281123/2946
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV8-281123/2947
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV8-281123/2948
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV8-281123/2949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-NSV8-281123/2950
Product: sm_9200					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2951
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2953
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2954
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2955
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2957
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2958
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2959
Product: sm_9250					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2960
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2961
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2962
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2964
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2965
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2966
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2968
Product: sm_9400					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2969
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2971
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2972
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2973
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2975
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2976
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2977
Product: sm_9450					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2978
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2979
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2980
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to a firewall crash. **CVE ID : CVE-2023-39277**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2982
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2983
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2984
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow	https://psirt.global.sonicwall.com/vuln-	H-SON-SM_9-281123/2985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	detail/SNWLID-2023-0012	
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2986
Product: sm_9600					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2987
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2989
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2990
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2991
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2993
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2994
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2995
Product: sm_9650					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2996
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2997
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2998
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/2999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/3000
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/3001
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/3002
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/3003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SM_9-281123/3004
Product: sohow					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3005
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3007
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3008
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3009
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3011
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3012
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3013
Product: soho_250					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3014
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3015
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3016
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3018
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3019
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3020
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3022
Product: soho_250w					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3023
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3025
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3026
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3027
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3029
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3030
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-SOHO-281123/3031
Product: tz270					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ27-281123/3032
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ27-281123/3033
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ27-281123/3034
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ27-281123/3035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ27-281123/3036
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ27-281123/3037
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ27-281123/3038
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ27-281123/3039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ27-281123/3040
Product: tz270w					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ27-281123/3041
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ27-281123/3042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ27-281123/3043
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ27-281123/3044
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ27-281123/3045
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ27-281123/3046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ27-281123/3047
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ27-281123/3048
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ27-281123/3049
Product: tz370					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ37-281123/3050
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ37-281123/3051
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ37-281123/3052
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ37-281123/3053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ37-281123/3054
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ37-281123/3055
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ37-281123/3056
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ37-281123/3057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ37-281123/3058
Product: tz370w					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ37-281123/3059
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ37-281123/3060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ37-281123/3061
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ37-281123/3062
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ37-281123/3063
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ37-281123/3064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ37-281123/3065
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ37-281123/3066
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ37-281123/3067
Product: tz470					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ47-281123/3068
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ47-281123/3069
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ47-281123/3070
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ47-281123/3071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ47-281123/3072
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ47-281123/3073
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ47-281123/3074
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ47-281123/3075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ47-281123/3076
Product: tz470w					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ47-281123/3077
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ47-281123/3078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ47-281123/3079
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ47-281123/3080
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ47-281123/3081
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ47-281123/3082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ47-281123/3083
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ47-281123/3084
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ47-281123/3085
Product: tz570					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3086
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3087
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3088
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3090
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3091
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3092
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3094
Product: tz570p					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3095
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3097
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3098
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3099
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3101
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3102
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3103
Product: tz570w					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3104
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3105
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3106
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3108
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3109
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3110
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ57-281123/3112
Product: tz670					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ67-281123/3113
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ67-281123/3114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ67-281123/3115
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ67-281123/3116
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ67-281123/3117
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ67-281123/3118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ67-281123/3119
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ67-281123/3120
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ67-281123/3121
Product: tz_300					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3122
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3123
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3124
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3126
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3127
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3128
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3130
Product: tz_300p					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3131
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3133
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3134
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3135
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3137
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3138
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3139
Product: tz_300w					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3140
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3141
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3142
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3144
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3145
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3146
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3148
Product: tz_350					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3149
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3151
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3152
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3153
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3155
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3156
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_3-281123/3157
Product: tz_400					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_4-281123/3158
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_4-281123/3159
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_4-281123/3160
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_4-281123/3161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_4-281123/3162
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_4-281123/3163
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_4-281123/3164
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_4-281123/3165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_4-281123/3166
Product: tz_400w					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_4-281123/3167
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_4-281123/3168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_4-281123/3169
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_4-281123/3170
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_4-281123/3171
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_4-281123/3172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_4-281123/3173
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_4-281123/3174
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_4-281123/3175
Product: tz_500					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_5-281123/3176
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_5-281123/3177
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_5-281123/3178
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_5-281123/3179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to a firewall crash. **CVE ID : CVE-2023-39277**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_5-281123/3180
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_5-281123/3181
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_5-281123/3182
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow	https://psirt.global.sonicwall.com/vuln-	H-SON-TZ_5-281123/3183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	detail/SNWLID-2023-0012	
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_5-281123/3184
Product: tz_500w					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_5-281123/3185
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_5-281123/3186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_5-281123/3187
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_5-281123/3188
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_5-281123/3189
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_5-281123/3190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_5-281123/3191
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_5-281123/3192
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_5-281123/3193
Product: tz_600					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_6-281123/3194
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_6-281123/3195
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_6-281123/3196
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_6-281123/3197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39277		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_6-281123/3198
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_6-281123/3199
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_6-281123/3200
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_6-281123/3201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_6-281123/3202
Product: tz_600p					
Affected Version(s): -					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_6-281123/3203
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_6-281123/3204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_6-281123/3205
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_6-281123/3206
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_6-281123/3207
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_6-281123/3208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_6-281123/3209
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_6-281123/3210
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	H-SON-TZ_6-281123/3211
Vendor: Synology					
Product: bc500					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	25-Oct-2023	9.8	A vulnerability regarding use of externally-controlled format string is found in the cgi component. This allows remote attackers to execute arbitrary code via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.5-0185 may be affected: BC500 and TC500. **CVE ID : CVE-2023-5746**	https://www.synology.com/en-global/security/advisory/Synology_SA_23_11	H-SYN-BC50-281123/3212
Product: tc500					
Affected Version(s): -					
Use of Externally-Controlled Format String	25-Oct-2023	9.8	A vulnerability regarding use of externally-controlled format string is found in the cgi component. This allows remote attackers to execute arbitrary code via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.5-0185 may be affected: BC500 and TC500.	https://www.synology.com/en-global/security/advisory/Synology_SA_23_11	H-SYN-TC50-281123/3213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5746		
Vendor: Tenda					
Product: w18e					
Affected Version(s): 1.0					
Out-of-bounds Write	25-Oct-2023	9.8	Tenda W18E V16.01.0.8(1576) contains a stack overflow vulnerability via the portMirrorMirroredPorts parameter in the formSetNetCheckTools function. **CVE ID : CVE-2023-46369**	N/A	H-TEN-W18E-281123/3214
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	Tenda W18E V16.01.0.8(1576) has a command injection vulnerability via the hostName parameter in the formSetNetCheckTools function. **CVE ID : CVE-2023-46370**	N/A	H-TEN-W18E-281123/3215
Vendor: totolink					
Product: a3300r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	31-Oct-2023	9.8	TOTOLINK A3300R 17.0.0cu.557_B20221024 contains a command injection via the file_name parameter in the UploadFirmwareFile function.	N/A	H-TOT-A330-281123/3216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			**CVE ID : CVE-2023-46976**		
Product: a3700r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	An issue in TOTOLINK A3700R v.9.1.2u.6165_20211012 allows a remote attacker to execute arbitrary code via the FileName parameter of the UploadFirmwareFile function. **CVE ID : CVE-2023-46574**	N/A	H-TOT-A370-281123/3217
Product: a7000r					
Affected Version(s): -					
Out-of-bounds Write	16-Oct-2023	9.8	TOTOLINK X5000R V9.1.0u.6118_B20201102 and TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the File parameter in the function UploadCustomModule. **CVE ID : CVE-2023-36947**	N/A	H-TOT-A700-281123/3218
Out-of-bounds Write	16-Oct-2023	9.8	TOTOLINK X5000R V9.1.0u.6118_B20201102 and TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to	N/A	H-TOT-A700-281123/3219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a stack overflow via the http_host parameter in the function loginAuth. **CVE ID : CVE-2023-36950**		
Out-of-bounds Write	16-Oct-2023	9.8	TOTOLINK X5000R V9.1.0u.6118_B20201102 and TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the lang parameter in the function setLanguageCfg. **CVE ID : CVE-2023-45984**	N/A	H-TOT-A700-281123/3220
Out-of-bounds Write	16-Oct-2023	7.5	TOTOLINK X5000R V9.1.0u.6118_B20201102 and TOTOLINK A7000R V9.1.0u.6115_B20201022 were discovered to contain a stack overflow in the function setParentalRules. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID : CVE-2023-45985**	N/A	H-TOT-A700-281123/3221
Product: cp300\+					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	16-Oct-2023	9.8	TOTOLINK CP300+ V5.2cu.7594_B20200910 was discovered to contain a stack overflow via the pingIp parameter in the function setDiagnosisCfg. **CVE ID : CVE-2023-36952**	N/A	H-TOT-CP30-281123/3222
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Oct-2023	9.8	TOTOLINK CP300+ V5.2cu.7594_B20200910 and before is vulnerable to command injection. **CVE ID : CVE-2023-36953**	N/A	H-TOT-CP30-281123/3223
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Oct-2023	9.8	TOTOLINK CP300+ V5.2cu.7594_B20200910 and before is vulnerable to command injection. **CVE ID : CVE-2023-36954**	N/A	H-TOT-CP30-281123/3224
Out-of-bounds Write	16-Oct-2023	9.8	TOTOLINK CP300+ <=V5.2cu.7594_B20200910 was discovered to contain a stack overflow via the File parameter in the function UploadCustomModule.	N/A	H-TOT-CP30-281123/3225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36955		
Product: lr1200gb					
Affected Version(s): -					
Out-of-bounds Write	31-Oct-2023	9.8	TOTOLINK LR1200GB V9.1.0u.6619_B20230130 was discovered to contain a stack overflow via the password parameter in the function loginAuth. **CVE ID : CVE-2023-46977**	N/A	H-TOT-LR12-281123/3226
Product: nr1800x					
Affected Version(s): -					
Out-of-bounds Write	16-Oct-2023	9.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain a stack overflow via the http_host parameter in the function loginAuth. **CVE ID : CVE-2023-36340**	N/A	H-TOT-NR18-281123/3227
Product: x2000r					
Affected Version(s): -					
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000RGh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formNtp.	N/A	H-TOT-X200-281123/3228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46540		
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formIpv6Setup. **CVE ID : CVE-2023-46541**	N/A	H-TOT-X200-281123/3229
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formMeshUploadConfig. **CVE ID : CVE-2023-46542**	N/A	H-TOT-X200-281123/3230
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formWlSiteSurvey. **CVE ID : CVE-2023-46543**	N/A	H-TOT-X200-281123/3231
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack	N/A	H-TOT-X200-281123/3232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow via the function formWirelessTbl. **CVE ID : CVE-2023-46544**		
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formWsc. **CVE ID : CVE-2023-46545**	N/A	H-TOT-X200-281123/3233
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formStats. **CVE ID : CVE-2023-46546**	N/A	H-TOT-X200-281123/3234
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formSysLog. **CVE ID : CVE-2023-46547**	N/A	H-TOT-X200-281123/3235
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to	N/A	H-TOT-X200-281123/3236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a stack overflow via the function formWlanRedirect. **CVE ID : CVE-2023-46548**		
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formSetLg. **CVE ID : CVE-2023-46549**	N/A	H-TOT-X200-281123/3237
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formMapDelDevice . **CVE ID : CVE-2023-46550**	N/A	H-TOT-X200-281123/3238
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formReflashClientTbl. **CVE ID : CVE-2023-46551**	N/A	H-TOT-X200-281123/3239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formMultiAP. **CVE ID : CVE-2023-46552**	N/A	H-TOT-X200-281123/3240
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formParentControl. **CVE ID : CVE-2023-46553**	N/A	H-TOT-X200-281123/3241
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formMapDel. **CVE ID : CVE-2023-46554**	N/A	H-TOT-X200-281123/3242
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formPortFw.	N/A	H-TOT-X200-281123/3243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46555		
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formFilter. **CVE ID : CVE-2023-46556**	N/A	H-TOT-X200-281123/3244
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formMultiAPVLAN. **CVE ID : CVE-2023-46557**	N/A	H-TOT-X200-281123/3245
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formMapDelDevice. **CVE ID : CVE-2023-46558**	N/A	H-TOT-X200-281123/3246
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the	N/A	H-TOT-X200-281123/3247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function formIPv6Addr. **CVE ID : CVE-2023-46559**		
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formTcpipSetup. **CVE ID : CVE-2023-46560**	N/A	H-TOT-X200-281123/3248
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formDosCfg. **CVE ID : CVE-2023-46562**	N/A	H-TOT-X200-281123/3249
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formIpQoS. **CVE ID : CVE-2023-46563**	N/A	H-TOT-X200-281123/3250
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was	N/A	H-TOT-X200-281123/3251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a stack overflow via the function formDMZ. **CVE ID : CVE-2023-46564**		
Product: x5000r					
Affected Version(s): -					
Out-of-bounds Write	16-Oct-2023	9.8	TOTOLINK X5000R V9.1.0u.6118_B20201102 and TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the File parameter in the function UploadCustomModule. **CVE ID : CVE-2023-36947**	N/A	H-TOT-X500-281123/3252
Out-of-bounds Write	16-Oct-2023	9.8	TOTOLINK X5000R V9.1.0u.6118_B20201102 and TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the http_host parameter in the function loginAuth. **CVE ID : CVE-2023-36950**	N/A	H-TOT-X500-281123/3253
Out-of-bounds Write	16-Oct-2023	9.8	TOTOLINK X5000R V9.1.0u.6118_B20201102 and TOTOLINK A7000R	N/A	H-TOT-X500-281123/3254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the lang parameter in the function setLanguageCfg. **CVE ID : CVE-2023-45984**		
Out-of-bounds Write	16-Oct-2023	7.5	TOTOLINK X5000R V9.1.0u.6118_B20201102 and TOTOLINK A7000R V9.1.0u.6115_B20201022 were discovered to contain a stack overflow in the function setParentalRules. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID : CVE-2023-45985**	N/A	H-TOT-X500-281123/3255
Product: x6000r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_ The 41DD80 function.	N/A	H-TOT-X600-281123/3256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46408		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_ 41CC04 function. **CVE ID : CVE-2023-46409**	N/A	H-TOT-X600-281123/3257
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_ The 416F60 function. **CVE ID : CVE-2023-46410**	N/A	H-TOT-X600-281123/3258
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_415258 function. **CVE ID : CVE-2023-46411**	N/A	H-TOT-X600-281123/3259
Improper Neutralization of Special Elements used in a Command	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via	N/A	H-TOT-X600-281123/3260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			the sub_41D998 function. **CVE ID : CVE-2023-46412**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_4155DC function. **CVE ID : CVE-2023-46413**	N/A	H-TOT-X600-281123/3261
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_ 41D494 function. **CVE ID : CVE-2023-46414**	N/A	H-TOT-X600-281123/3262
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_41E588 function. **CVE ID : CVE-2023-46415**	N/A	H-TOT-X600-281123/3263
Improper Neutralizat	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B202	N/A	H-TOT-X600-281123/3264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			30116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_ The 41A414 function. **CVE ID : CVE-2023-46416**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_415498 function. **CVE ID : CVE-2023-46417**	N/A	H-TOT-X600-281123/3265
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_412688 function. **CVE ID : CVE-2023-46418**	N/A	H-TOT-X600-281123/3266
Improper Neutralization of Special Elements used in a Command ('Comman	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via	N/A	H-TOT-X600-281123/3267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			the sub_415730 function. **CVE ID : CVE-2023-46419**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_41590C function. **CVE ID : CVE-2023-46420**	N/A	H-TOT-X600-281123/3268
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_411D00 function. **CVE ID : CVE-2023-46421**	N/A	H-TOT-X600-281123/3269
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_411994 function. **CVE ID : CVE-2023-46422**	N/A	H-TOT-X600-281123/3270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_417094 function. **CVE ID : CVE-2023-46423**	N/A	H-TOT-X600-281123/3271
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_422BD4 function. **CVE ID : CVE-2023-46424**	N/A	H-TOT-X600-281123/3272
Improper Neutralization of Special Elements used in a Command ('Command Injection')	31-Oct-2023	9.8	TOTOLINK X6000R V9.4.0cu.852_B20230719 was discovered to contain a command injection vulnerability via the enable parameter in the setLedCfg function. **CVE ID : CVE-2023-46979**	N/A	H-TOT-X600-281123/3273
Missing Authentication for Critical Function	31-Oct-2023	7.5	TOTOLINK X6000R V9.4.0cu.852_B20230719 is vulnerable to Incorrect Access Control.Attackers	N/A	H-TOT-X600-281123/3274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can reset login password & WIFI passwords without authentication. **CVE ID : CVE-2023-46978**		
Vendor: Tp-link					
Product: tl-wdr7660					
Affected Version(s): -					
Out-of-bounds Write	25-Oct-2023	9.8	TP-Link device TL-WDR7660 2.0.30 has a stack overflow vulnerability via the function upgradeInfoJsonToBin. **CVE ID : CVE-2023-46371**	N/A	H-TP--TL-W-281123/3275
Out-of-bounds Write	25-Oct-2023	9.8	TP-Link TL-WDR7660 2.0.30 has a stack overflow vulnerability via the function deviceInfoJsonToBincauses. **CVE ID : CVE-2023-46373**	N/A	H-TP--TL-W-281123/3276
Product: tl-wr886n					
Affected Version(s): 7.0					
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function	N/A	H-TP--TL-W-281123/3277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uninstallPluginReq Handle. **CVE ID : CVE-2023-46520**		
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function RegisterRegister. **CVE ID : CVE-2023-46521**	N/A	H-TP--TL-W-281123/3278
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function deviceInfoRegister. **CVE ID : CVE-2023-46522**	N/A	H-TP--TL-W-281123/3279
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function upgradeInfoRegister. **CVE ID : CVE-2023-46523**	N/A	H-TP--TL-W-281123/3280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function loginRegister. **CVE ID : CVE-2023-46525**	N/A	H-TP--TL-W-281123/3281
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function resetCloudPwdRegister. **CVE ID : CVE-2023-46526**	N/A	H-TP--TL-W-281123/3282
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function bindRequestHandle. **CVE ID : CVE-2023-46527**	N/A	H-TP--TL-W-281123/3283
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908	N/A	H-TP--TL-W-281123/3284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			n.bin was discovered to contain a stack overflow via the function modifyAccPwdRegister. **CVE ID : CVE-2023-46534**		
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function getResetVeriRegister. **CVE ID : CVE-2023-46535**	N/A	H-TP--TL-W-281123/3285
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function chkRegVeriRegister. **CVE ID : CVE-2023-46536**	N/A	H-TP--TL-W-281123/3286
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack	N/A	H-TP--TL-W-281123/3287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow via the function getRegVeriRegister. **CVE ID : CVE-2023-46537**		
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function chkResetVeriRegister. **CVE ID : CVE-2023-46538**	N/A	H-TP--TL-W-281123/3288
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function registerRequestHandle. **CVE ID : CVE-2023-46539**	N/A	H-TP--TL-W-281123/3289
Vendor: ui					
Product: unifi_dream_machine					
Affected Version(s): -					
N/A	25-Oct-2023	5.3	Instances of UniFi Network Application that (i) are run on a UniFi Gateway Console, and (ii) are	https://community.ui.com/releases/Security-Advisory-Bulletin-036-036/81367bc9-	H-UI-UNIF-281123/3290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 7.5.176. and earlier, implement device adoption with improper access control logic, creating a risk of access to device configuration information by a malicious actor with preexisting access to the network. Affected Products: UDM UDM-PRO UDM-SE UDR UDW Mitigation: Update UniFi Network to Version 7.5.187 or later. **CVE ID : CVE-2023-41721**	2a64-4435-95dc-bbe482457615	
Product: unifi_dream_machine_pro					
Affected Version(s): -					
N/A	25-Oct-2023	5.3	Instances of UniFi Network Application that (i) are run on a UniFi Gateway Console, and (ii) are versions 7.5.176. and earlier,	https://community.ui.com/releases/Security-Advisory-Bulletin-036-036/81367bc9-2a64-4435-	H-UI-UNIF-281123/3291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implement device adoption with improper access control logic, creating a risk of access to device configuration information by a malicious actor with preexisting access to the network. Affected Products: UDM UDM-PRO UDM-SE UDR UDW Mitigation: Update UniFi Network to Version 7.5.187 or later. **CVE ID : CVE-2023-41721**	95dc-bbe482457615	
Product: unifi_dream_machine_special_edition					
Affected Version(s): -					
N/A	25-Oct-2023	5.3	Instances of UniFi Network Application that (i) are run on a UniFi Gateway Console, and (ii) are versions 7.5.176. and earlier, implement device adoption with	https://community.ui.com/releases/Security-Advisory-Bulletin-036-036/81367bc9-2a64-4435-95dc-bbe482457615	H-UI-UNIF-281123/3292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper access control logic, creating a risk of access to device configuration information by a malicious actor with preexisting access to the network. Affected Products: UDM UDM-PRO UDM-SE UDR UDW Mitigation: Update UniFi Network to Version 7.5.187 or later. **CVE ID : CVE-2023-41721**		
Product: unifi_dream_router					
Affected Version(s): -					
N/A	25-Oct-2023	5.3	Instances of UniFi Network Application that (i) are run on a UniFi Gateway Console, and (ii) are versions 7.5.176. and earlier, implement device adoption with improper access control logic,	https://community.ui.com/releases/Security-Advisory-Bulletin-036-036/81367bc9-2a64-4435-95dc-bbe482457615	H-UI-UNIF-281123/3293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			creating a risk of access to device configuration information by a malicious actor with preexisting access to the network. Affected Products: UDM UDM-PRO UDM-SE UDR UDW Mitigation: Update UniFi Network to Version 7.5.187 or later. **CVE ID : CVE-2023-41721**		
Product: unifi_dream_wall					
Affected Version(s): -					
N/A	25-Oct-2023	5.3	Instances of UniFi Network Application that (i) are run on a UniFi Gateway Console, and (ii) are versions 7.5.176. and earlier, implement device adoption with improper access control logic, creating a risk of access to device	https://community.ui.com/releases/Security-Advisory-Bulletin-036-036/81367bc9-2a64-4435-95dc-bbe482457615	H-UI-UNIF-281123/3294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration information by a malicious actor with preexisting access to the network. Affected Products: UDM UDM-PRO UDM-SE UDR UDW Mitigation: Update UniFi Network to Version 7.5.187 or later. **CVE ID : CVE-2023-41721**		
Vendor: viessmann					
Product: vitogate_300					
Affected Version(s): -					
Direct Request ('Forced Browsing')	23-Oct-2023	6.5	A vulnerability was found in Viessmann Vitogate 300 up to 2.1.3.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /cgi-bin/. The manipulation leads to direct request. The exploit has	N/A	H-VIE-VITO-281123/3295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. The identifier of this vulnerability is VDB-243140. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-5702**		
Vendor: Wago					
Product: compact_controller_100					
Affected Version(s): -					
Externally Controlled Reference to a Resource in Another Sphere	17-Oct-2023	2.7	On affected Wago products an remote attacker with administrative privileges can access files to which he has already access to through an undocumented local file inclusion. This access is logged in a different log file than expected. **CVE ID : CVE-2023-4089**	N/A	H-WAG-COMP-281123/3296
Product: edge_controller					
Affected Version(s): -					
Externally Controlled Reference to a	17-Oct-2023	2.7	On affected Wago products an remote attacker with	N/A	H-WAG-EDGE-281123/3297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource in Another Sphere			administrative privileges can access files to which he has already access to through an undocumented local file inclusion. This access is logged in a different log file than expected. **CVE ID : CVE-2023-4089**		
Product: pfc100					
Affected Version(s): -					
Externally Controlled Reference to a Resource in Another Sphere	17-Oct-2023	2.7	On affected Wago products an remote attacker with administrative privileges can access files to which he has already access to through an undocumented local file inclusion. This access is logged in a different log file than expected. **CVE ID : CVE-2023-4089**	N/A	H-WAG-PFC1-281123/3298
Product: pfc200					
Affected Version(s): -					
Externally Controlled Reference to a Resource	17-Oct-2023	2.7	On affected Wago products an remote attacker with administrative	N/A	H-WAG-PFC2-281123/3299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
in Another Sphere			privileges can access files to which he has already access to through an undocumented local file inclusion. This access is logged in a different log file than expected. **CVE ID : CVE-2023-4089**		
Product: touch_panel_600_advanced					
Affected Version(s): -					
Externally Controlled Reference to a Resource in Another Sphere	17-Oct-2023	2.7	On affected Wago products an remote attacker with administrative privileges can access files to which he has already access to through an undocumented local file inclusion. This access is logged in a different log file than expected. **CVE ID : CVE-2023-4089**	N/A	H-WAG-TOUC-281123/3300
Product: touch_panel_600_marine					
Affected Version(s): -					
Externally Controlled Reference to a Resource	17-Oct-2023	2.7	On affected Wago products an remote attacker with administrative privileges can	N/A	H-WAG-TOUC-281123/3301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
in Another Sphere			access files to which he has already access to through an undocumented local file inclusion. This access is logged in a different log file than expected. **CVE ID : CVE-2023-4089**		
Product: touch_panel_600_standard					
Affected Version(s): -					
Externally Controlled Reference to a Resource in Another Sphere	17-Oct-2023	2.7	On affected Wago products an remote attacker with administrative privileges can access files to which he has already access to through an undocumented local file inclusion. This access is logged in a different log file than expected. **CVE ID : CVE-2023-4089**	N/A	H-WAG-TOUC-281123/3302
Vendor: weintek					
Product: cmt-fhd					
Affected Version(s): -					
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin command_wb.cgi contains a stack-	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT--281123/3303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-38584**		
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin codesys.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-43492**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT--281123/3304
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Oct-2023	8.8	In Weintek's cMT3000 HMI Web CGI device, an anonymous attacker can execute arbitrary commands after login to the device. **CVE ID : CVE-2023-40145**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT--281123/3305
Product: cmt-hdm					
Affected Version(s): -					
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-	https://dl.weintek.com/public/Document/TEC	H-WEI-CMT--281123/3306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin command_wb.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-38584**	/TEC23005E_cMT_Web_Security_Update.pdf	
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin codesys.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-43492**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT--281123/3307
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Oct-2023	8.8	In Weintek's cMT3000 HMI Web CGI device, an anonymous attacker can execute arbitrary commands after login to the device. **CVE ID : CVE-2023-40145**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT--281123/3308
Product: cmt3071					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin command_wb.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-38584**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT3-281123/3309
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin codesys.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-43492**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT3-281123/3310
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Oct-2023	8.8	In Weintek's cMT3000 HMI Web CGI device, an anonymous attacker can execute arbitrary commands after login to the device. **CVE ID : CVE-2023-40145**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT3-281123/3311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: cmt3072					
Affected Version(s): -					
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin command_wb.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-38584**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT3-281123/3312
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin codesys.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-43492**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT3-281123/3313
Improper Neutralization of Special Elements used in an OS Command ('OS	19-Oct-2023	8.8	In Weintek's cMT3000 HMI Web CGI device, an anonymous attacker can execute arbitrary commands after login to the device.	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT3-281123/3314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			**CVE ID : CVE-2023-40145**		
Product: cmt3090					
Affected Version(s): -					
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin command_wb.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-38584**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT3-281123/3315
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin codesys.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-43492**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT3-281123/3316
Improper Neutralization of Special	19-Oct-2023	8.8	In Weintek's cMT3000 HMI Web CGI device, an anonymous	https://dl.weintek.com/public/Document/TEC/TEC23005E_c	H-WEI-CMT3-281123/3317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			attacker can execute arbitrary commands after login to the device. **CVE ID : CVE-2023-40145**	MT_Web_Security_Update.pdf	
Product: cmt3103					
Affected Version(s): -					
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin command_wb.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-38584**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT3-281123/3318
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin codesys.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-43492**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT3-281123/3319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Oct-2023	8.8	In Weintek's cMT3000 HMI Web CGI device, an anonymous attacker can execute arbitrary commands after login to the device. **CVE ID : CVE-2023-40145**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT3-281123/3320
Product: cmt3151					
Affected Version(s): -					
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin command_wb.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-38584**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT3-281123/3321
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin codesys.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT3-281123/3322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass login authentication. **CVE ID : CVE-2023-43492**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Oct-2023	8.8	In Weintek's cMT3000 HMI Web CGI device, an anonymous attacker can execute arbitrary commands after login to the device. **CVE ID : CVE-2023-40145**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	H-WEI-CMT3-281123/3323
Vendor: Yealink					
Product: sip-t19p-e2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Oct-2023	8.8	An issue in YeaLinkSIP-T19P-E2 v.53.84.0.15 allows a remote privileged attacker to execute arbitrary code via a crafted request the ping function of the diagnostic component. **CVE ID : CVE-2023-43959**	N/A	H-YEA-SIP--281123/3324
Vendor: zioncom					
Product: a7000r					
Affected Version(s): -					
N/A	27-Oct-2023	9.8	An issue in ZIONCOM (Hong Kong) Technology Limited A7000R	N/A	H-ZIO-A700-281123/3325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v.4.1cu.4154 allows an attacker to execute arbitrary code via the cig-bin/cstecgi.cgi to the settings/setPasswordCfg function. **CVE ID : CVE-2023-46510**		
Operating System					
Vendor: airtel					
Product: dragon_path_707gr1_firmware					
Affected Version(s): * Up to (including) 2023-10-22					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-2023	4.8	A vulnerability classified as problematic has been found in Dragon Path 707GR1 up to 20231022. Affected is an unknown function of the component Ping Diagnostics. The manipulation of the argument Host Address with the input >><img/src/onerror=alert(1)> 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-243594 is the identifier	N/A	O-AIR-DRAG-281123/3326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. **CVE ID : CVE-2023-5789**		
Vendor: Apple					
Product: ipados					
Affected Version(s): * Up to (excluding) 16.7.2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2023-40447**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	O-APP-IPAD-281123/3327
Use After Free	25-Oct-2023	8.8	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support	O-APP-IPAD-281123/3328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to arbitrary code execution. **CVE ID : CVE-2023-41976**	.apple.com/en-us/HT213984	
N/A	25-Oct-2023	8.8	A logic issue was addressed with improved checks. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2023-42852**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	O-APP-IPAD-281123/3329
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-40423**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	O-APP-IPAD-281123/3330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-42841**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-IPAD-281123/3331
N/A	25-Oct-2023	7.5	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 16.7.2 and iPadOS 16.7.2. A user's password may be read aloud by VoiceOver. **CVE ID : CVE-2023-32359**	https://support.apple.com/en-us/HT213981	O-APP-IPAD-281123/3332
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-	O-APP-IPAD-281123/3333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13.6.1, macOS Sonoma 14.1. Processing an image may result in disclosure of process memory. **CVE ID : CVE-2023-40416**	us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, Safari 17.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Processing web content may lead to a denial-of-service. **CVE ID : CVE-2023-41983**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213984	O-APP-IPAD-281123/3334
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An attacker that has already achieved kernel code execution may be able to bypass kernel	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985	O-APP-IPAD-281123/3335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory mitigations. **CVE ID : CVE-2023-42849**		
N/A	25-Oct-2023	5.5	The issue was addressed with improved handling of caches. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to read sensitive location information. **CVE ID : CVE-2023-40413**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985	O-APP-IPAD-281123/3336
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to cause a denial-of-service. **CVE ID : CVE-2023-40449**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	O-APP-IPAD-281123/3337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	25-Oct-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to access sensitive user data. **CVE ID : CVE-2023-41254**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	O-APP-IPAD-281123/3338
N/A	25-Oct-2023	5.3	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Hide My Email may be deactivated unexpectedly. **CVE ID : CVE-2023-40408**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-IPAD-281123/3339
N/A	25-Oct-2023	5.3	This issue was addressed by removing the vulnerable code. This issue is fixed in watchOS 10.1, iOS 16.7.2 and	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support	O-APP-IPAD-281123/3340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 16.7.2, tvOS 17.1, iOS 17.1 and iPadOS 17.1. A device may be passively tracked by its Wi-Fi MAC address. **CVE ID : CVE-2023-42846**	.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213987, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	
N/A	25-Oct-2023	4.6	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data. **CVE ID : CVE-2023-41982**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-IPAD-281123/3341
N/A	25-Oct-2023	4.6	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/	O-APP-IPAD-281123/3342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Siri to access sensitive user data. **CVE ID : CVE-2023-41997**	HT213981, https://support.apple.com/kb/HT213982	
N/A	25-Oct-2023	4.3	The issue was addressed with improved handling of caches. This issue is fixed in macOS Sonoma 14.1, iOS 16.7.2 and iPadOS 16.7.2. Visiting a malicious website may reveal browsing history. **CVE ID : CVE-2023-41977**	https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213984	O-APP-IPAD-281123/3343
Affected Version(s): * Up to (excluding) 17.1					
Insertion of Sensitive Information into Log File	25-Oct-2023	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An app may be able to access sensitive user data. **CVE ID : CVE-2023-42857**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213982, https://support.apple.com/kb/HT213984	O-APP-IPAD-281123/3344
Affected Version(s): From (including) 17.0 Up to (excluding) 17.1					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-	O-APP-IPAD-281123/3345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2023-40447**	us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	
Use After Free	25-Oct-2023	8.8	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2023-41976**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	O-APP-IPAD-281123/3346
N/A	25-Oct-2023	8.8	A logic issue was addressed with improved checks. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-	O-APP-IPAD-281123/3347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to arbitrary code execution. **CVE ID : CVE-2023-42852**	us/HT213987, https://support.apple.com/en-us/HT213984	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-40423**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	O-APP-IPAD-281123/3348
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-42841**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-IPAD-281123/3349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Oct-2023	7.5	The issue was addressed with improved UI handling. This issue is fixed in iOS 17.1 and iPadOS 17.1. A device may persistently fail to lock. **CVE ID : CVE-2023-40445**	https://support.apple.com/en-us/HT213982, https://support.apple.com/kb/HT213982	O-APP-IPAD-281123/3350
N/A	25-Oct-2023	7.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An attacker may be able to access passkeys without authentication. **CVE ID : CVE-2023-42847**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213982, https://support.apple.com/kb/HT213984	O-APP-IPAD-281123/3351
N/A	25-Oct-2023	6.8	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data. **CVE ID : CVE-2023-41988**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213982, https://support.apple.com/kb/HT213984, https://support.apple.com/kb/HT213988	O-APP-IPAD-281123/3352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. Processing an image may result in disclosure of process memory. **CVE ID : CVE-2023-40416**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	O-APP-IPAD-281123/3353
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, Safari 17.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Processing web content may lead to a denial-of-service. **CVE ID : CVE-2023-41983**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213984	O-APP-IPAD-281123/3354
Improper Restriction of Operations within the Bounds of	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1,	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-	O-APP-IPAD-281123/3355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations. **CVE ID : CVE-2023-42849**	us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985	
N/A	25-Oct-2023	5.5	The issue was addressed with improved handling of caches. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to read sensitive location information. **CVE ID : CVE-2023-40413**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985	O-APP-IPAD-281123/3356
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981,	O-APP-IPAD-281123/3357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to cause a denial-of-service. **CVE ID : CVE-2023-40449**	https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	
N/A	25-Oct-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An app may be able to access sensitive user data. **CVE ID : CVE-2023-41072**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213982, https://support.apple.com/kb/HT213984	O-APP-IPAD-281123/3358
Insertion of Sensitive Information into Log File	25-Oct-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to access sensitive user data. **CVE ID : CVE-2023-41254**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	O-APP-IPAD-281123/3359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Oct-2023	5.3	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Hide My Email may be deactivated unexpectedly. **CVE ID : CVE-2023-40408**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-IPAD-281123/3360
Missing Authentication for Critical Function	25-Oct-2023	5.3	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. Photos in the Hidden Photos Album may be viewed without authentication. **CVE ID : CVE-2023-42845**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213982, https://support.apple.com/kb/HT213984	O-APP-IPAD-281123/3361
N/A	25-Oct-2023	5.3	This issue was addressed by removing the vulnerable code. This issue is fixed in watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, tvOS 17.1, iOS 17.1 and	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988,	O-APP-IPAD-281123/3362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 17.1. A device may be passively tracked by its Wi-Fi MAC address. **CVE ID : CVE-2023-42846**	https://support.apple.com/en-us/HT213987, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	
N/A	25-Oct-2023	4.6	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data. **CVE ID : CVE-2023-41982**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-IPAD-281123/3363
N/A	25-Oct-2023	4.6	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data.	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support	O-APP-IPAD-281123/3364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-41997	.apple.com/kb/HT213982	
Product: iphone_os					
Affected Version(s): * Up to (excluding) 16.7.2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2023-40447**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	O-APP-IPHO-281123/3365
Use After Free	25-Oct-2023	8.8	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2023-41976**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	O-APP-IPHO-281123/3366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Oct-2023	8.8	A logic issue was addressed with improved checks. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2023-42852**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	O-APP-IPHO-281123/3367
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-40423**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	O-APP-IPHO-281123/3368
Improper Restriction of Operations within the Bounds of	25-Oct-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981,	O-APP-IPHO-281123/3369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			14.1, iOS 17.1 and iPadOS 17.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-42841**	https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	
N/A	25-Oct-2023	7.5	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 16.7.2 and iPadOS 16.7.2. A user's password may be read aloud by VoiceOver. **CVE ID : CVE-2023-32359**	https://support.apple.com/en-us/HT213981	O-APP-IPHO-281123/3370
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. Processing an image may result in disclosure of process memory.	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support	O-APP-IPHO-281123/3371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-40416	.apple.com/kb/HT213981	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, Safari 17.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Processing web content may lead to a denial-of-service. **CVE ID : CVE-2023-41983**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213984	O-APP-IPHO-281123/3372
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations. **CVE ID : CVE-2023-42849**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985	O-APP-IPHO-281123/3373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Oct-2023	5.5	The issue was addressed with improved handling of caches. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to read sensitive location information. **CVE ID : CVE-2023-40413**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985	O-APP-IPHO-281123/3374
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to cause a denial-of-service. **CVE ID : CVE-2023-40449**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	O-APP-IPHO-281123/3375
Insertion of Sensitive Information into Log File	25-Oct-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981,	O-APP-IPHO-281123/3376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to access sensitive user data. **CVE ID : CVE-2023-41254**	https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	
N/A	25-Oct-2023	5.3	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Hide My Email may be deactivated unexpectedly. **CVE ID : CVE-2023-40408**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-IPHO-281123/3377
N/A	25-Oct-2023	5.3	This issue was addressed by removing the vulnerable code. This issue is fixed in watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, tvOS 17.1, iOS 17.1 and iPadOS 17.1. A device may be passively tracked	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213987, https://support	O-APP-IPHO-281123/3378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by its Wi-Fi MAC address. **CVE ID : CVE-2023-42846**	.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	
N/A	25-Oct-2023	4.6	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data. **CVE ID : CVE-2023-41982**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-IPHO-281123/3379
N/A	25-Oct-2023	4.6	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data. **CVE ID : CVE-2023-41997**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-IPHO-281123/3380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Oct-2023	4.3	The issue was addressed with improved handling of caches. This issue is fixed in macOS Sonoma 14.1, iOS 16.7.2 and iPadOS 16.7.2. Visiting a malicious website may reveal browsing history. **CVE ID : CVE-2023-41977**	https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213984	O-APP-IPHO-281123/3381
Affected Version(s): * Up to (excluding) 17.1					
Insertion of Sensitive Information into Log File	25-Oct-2023	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An app may be able to access sensitive user data. **CVE ID : CVE-2023-42857**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213982, https://support.apple.com/kb/HT213984	O-APP-IPHO-281123/3382
Affected Version(s): From (including) 17.0 Up to (excluding) 17.1					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support	O-APP-IPHO-281123/3383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			content may lead to arbitrary code execution. **CVE ID : CVE-2023-40447**	.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	
Use After Free	25-Oct-2023	8.8	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2023-41976**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	O-APP-IPHO-281123/3384
N/A	25-Oct-2023	8.8	A logic issue was addressed with improved checks. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2023-42852**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	O-APP-IPHO-281123/3385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-40423**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	O-APP-IPHO-281123/3386
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-42841**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-IPHO-281123/3387
N/A	25-Oct-2023	7.5	The issue was addressed with improved UI handling. This issue is fixed in iOS 17.1 and iPadOS	https://support.apple.com/en-us/HT213982, https://support.apple.com/kb/HT213982	O-APP-IPHO-281123/3388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			17.1. A device may persistently fail to lock. **CVE ID : CVE-2023-40445**		
N/A	25-Oct-2023	7.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An attacker may be able to access passkeys without authentication. **CVE ID : CVE-2023-42847**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213982, https://support.apple.com/kb/HT213984	O-APP-IPHO-281123/3389
N/A	25-Oct-2023	6.8	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data. **CVE ID : CVE-2023-41988**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213982, https://support.apple.com/kb/HT213984, https://support.apple.com/kb/HT213988	O-APP-IPHO-281123/3390
Improper Restriction of Operations within the Bounds of	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983,	O-APP-IPHO-281123/3391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. Processing an image may result in disclosure of process memory. **CVE ID : CVE-2023-40416**	https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, Safari 17.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Processing web content may lead to a denial-of-service. **CVE ID : CVE-2023-41983**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213984	O-APP-IPHO-281123/3392
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An attacker	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-	O-APP-IPHO-281123/3393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that has already achieved kernel code execution may be able to bypass kernel memory mitigations. **CVE ID : CVE-2023-42849**	us/HT213984, https://support.apple.com/en-us/HT213985	
N/A	25-Oct-2023	5.5	The issue was addressed with improved handling of caches. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to read sensitive location information. **CVE ID : CVE-2023-40413**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985	O-APP-IPHO-281123/3394
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985,	O-APP-IPHO-281123/3395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial-of-service. **CVE ID : CVE-2023-40449**	https://support.apple.com/kb/HT213981	
N/A	25-Oct-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An app may be able to access sensitive user data. **CVE ID : CVE-2023-41072**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213982, https://support.apple.com/kb/HT213984	O-APP-IPHO-281123/3396
Insertion of Sensitive Information into Log File	25-Oct-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to access sensitive user data. **CVE ID : CVE-2023-41254**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	O-APP-IPHO-281123/3397
N/A	25-Oct-2023	5.3	An inconsistent user interface issue was addressed with improved state management. This issue is fixed	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981,	O-APP-IPHO-281123/3398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Hide My Email may be deactivated unexpectedly. **CVE ID : CVE-2023-40408**	https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	
Missing Authentication for Critical Function	25-Oct-2023	5.3	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. Photos in the Hidden Photos Album may be viewed without authentication. **CVE ID : CVE-2023-42845**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213982, https://support.apple.com/kb/HT213984	O-APP-IPHO-281123/3399
N/A	25-Oct-2023	5.3	This issue was addressed by removing the vulnerable code. This issue is fixed in watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, tvOS 17.1, iOS 17.1 and iPadOS 17.1. A device may be passively tracked by its Wi-Fi MAC address.	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213987, https://support.apple.com/kb/HT213981,	O-APP-IPHO-281123/3400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-42846	https://support.apple.com/kb/HT213982	
N/A	25-Oct-2023	4.6	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data. **CVE ID : CVE-2023-41982**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-IPHO-281123/3401
N/A	25-Oct-2023	4.6	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data. **CVE ID : CVE-2023-41997**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-IPHO-281123/3402
Product: macos					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	27-Oct-2023	7.8	VMware Tools contains a local privilege escalation vulnerability. A malicious actor with local user access to a guest virtual machine may elevate privileges within the virtual machine. **CVE ID : CVE-2023-34057**	https://www.vmware.com/security/advisories/VMSA-2023-0024.html	O-APP-MACO-281123/3403
N/A	25-Oct-2023	4.3	A website could have obscured the full screen notification by using the file open dialog. This could have led to user confusion and possible spoofing attacks. *Note: This issue only affected macOS operating systems. Other operating systems are unaffected.* This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5726**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1846205	O-APP-MACO-281123/3404
Affected Version(s): 14.0					
Use After Free	25-Oct-2023	7.8	A use-after-free issue was addressed with	https://support.apple.com/en-us/HT213984,	O-APP-MACO-281123/3405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved memory management. This issue is fixed in macOS Sonoma 14.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-40404**	https://support.apple.com/kb/HT213984	
N/A	25-Oct-2023	5.3	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Hide My Email may be deactivated unexpectedly. **CVE ID : CVE-2023-40408**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-MACO-281123/3406
Insertion of Sensitive Information into Log File	25-Oct-2023	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.1. An app may be able to read sensitive location information. **CVE ID : CVE-2023-40405**	https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213984	O-APP-MACO-281123/3407
Affected Version(s): From (including) 12.0 Up to (excluding) 12.7.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. Processing a file may lead to unexpected app termination or arbitrary code execution. **CVE ID : CVE-2023-42856**	https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213983, https://support.apple.com/kb/HT213984, https://support.apple.com/kb/HT213985	O-APP-MACO-281123/3408
N/A	25-Oct-2023	5.5	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. An app may be able to cause a denial-of-service to Endpoint Security clients. **CVE ID : CVE-2023-42854**	https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213983, https://support.apple.com/kb/HT213984, https://support.apple.com/kb/HT213985	O-APP-MACO-281123/3409
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.7.1					
Improper Restriction of Operations within the Bounds of	25-Oct-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983,	O-APP-MACO-281123/3410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-40423**	https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	
Improper Link Resolution Before File Access ('Link Following')	25-Oct-2023	7.5	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. A website may be able to access sensitive user data when resolving symlinks. **CVE ID : CVE-2023-42844**	https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213983, https://support.apple.com/kb/HT213984, https://support.apple.com/kb/HT213985	O-APP-MACO-281123/3411
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984,	O-APP-MACO-281123/3412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sonoma 14.1. Processing an image may result in disclosure of process memory. **CVE ID : CVE-2023-40416**	https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations. **CVE ID : CVE-2023-42849**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985	O-APP-MACO-281123/3413
N/A	25-Oct-2023	5.5	The issue was addressed with improved handling of caches. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support	O-APP-MACO-281123/3414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			14.1. An app may be able to read sensitive location information. **CVE ID : CVE-2023-40413**	.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985	
N/A	25-Oct-2023	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. An app may be able to access sensitive user data. **CVE ID : CVE-2023-40421**	https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213983, https://support.apple.com/kb/HT213984, https://support.apple.com/kb/HT213985	O-APP-MACO-281123/3415
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to cause a denial-of-service. **CVE ID : CVE-2023-40449**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	O-APP-MACO-281123/3416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	25-Oct-2023	4.4	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Monterey 12.7.1. An app with root privileges may be able to access private information. **CVE ID : CVE-2023-40425**	https://support.apple.com/en-us/HT213983, https://support.apple.com/kb/HT213983	O-APP-MACO-281123/3417
N/A	25-Oct-2023	4.3	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. A website may be able to access the microphone without the microphone use indicator being shown. **CVE ID : CVE-2023-41975**	https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213983, https://support.apple.com/kb/HT213984, https://support.apple.com/kb/HT213985	O-APP-MACO-281123/3418
Affected Version(s): From (including) 13.0 Up to (excluding) 13.6.1					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1,	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-	O-APP-MACO-281123/3419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-40423**	us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-42841**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-MACO-281123/3420
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. Processing a file may lead to unexpected app termination or	https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213983, https://support.apple.com/kb/	O-APP-MACO-281123/3421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2023-42856**	HT213984, https://support.apple.com/kb/HT213985	
Missing Authentication for Critical Function	25-Oct-2023	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.6.1. An attacker may be able to access passkeys without authentication. **CVE ID : CVE-2023-40401**	https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213985	O-APP-MACO-281123/3422
Improper Link Resolution Before File Access ('Link Following')	25-Oct-2023	7.5	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. A website may be able to access sensitive user data when resolving symlinks. **CVE ID : CVE-2023-42844**	https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213983, https://support.apple.com/kb/HT213984, https://support.apple.com/kb/HT213985	O-APP-MACO-281123/3423
Improper Restriction of Operations within the Bounds of	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support	O-APP-MACO-281123/3424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. Processing an image may result in disclosure of process memory. **CVE ID : CVE-2023-40416**	.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations. **CVE ID : CVE-2023-42849**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985	O-APP-MACO-281123/3425
N/A	25-Oct-2023	5.5	The issue was addressed with improved handling of caches. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1,	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-	O-APP-MACO-281123/3426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to read sensitive location information. **CVE ID : CVE-2023-40413**	us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985	
N/A	25-Oct-2023	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. An app may be able to access sensitive user data. **CVE ID : CVE-2023-40421**	https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213983, https://support.apple.com/kb/HT213984, https://support.apple.com/kb/HT213985	O-APP-MACO-281123/3427
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-	O-APP-MACO-281123/3428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial-of-service. **CVE ID : CVE-2023-40449**	us/HT213985, https://support.apple.com/kb/HT213981	
N/A	25-Oct-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.6.1. An app may be able to access protected user data. **CVE ID : CVE-2023-41077**	https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213985	O-APP-MACO-281123/3429
Insertion of Sensitive Information into Log File	25-Oct-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to access sensitive user data. **CVE ID : CVE-2023-41254**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	O-APP-MACO-281123/3430
N/A	25-Oct-2023	5.5	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura	https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985,	O-APP-MACO-281123/3431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13.6.1. An app may be able to cause a denial-of-service to Endpoint Security clients. **CVE ID : CVE-2023-42854**	https://support.apple.com/kb/HT213983, https://support.apple.com/kb/HT213984, https://support.apple.com/kb/HT213985	
N/A	25-Oct-2023	4.3	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. A website may be able to access the microphone without the microphone use indicator being shown. **CVE ID : CVE-2023-41975**	https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213983, https://support.apple.com/kb/HT213984, https://support.apple.com/kb/HT213985	O-APP-MACO-281123/3432
Affected Version(s): From (including) 14.0 Up to (excluding) 14.1					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-	O-APP-MACO-281123/3433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to arbitrary code execution. **CVE ID : CVE-2023-40447**	us/HT213987, https://support.apple.com/en-us/HT213984	
Use After Free	25-Oct-2023	8.8	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2023-41976**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	O-APP-MACO-281123/3434
N/A	25-Oct-2023	8.8	A logic issue was addressed with improved checks. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2023-42852**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	O-APP-MACO-281123/3435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-40423**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	O-APP-MACO-281123/3436
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-42841**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-MACO-281123/3437
Improper Restriction of Operations within the Bounds of	25-Oct-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma	https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213984,	O-APP-MACO-281123/3438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. Processing a file may lead to unexpected app termination or arbitrary code execution. **CVE ID : CVE-2023-42856**	https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213983, https://support.apple.com/kb/HT213984, https://support.apple.com/kb/HT213985	
Improper Link Resolution Before File Access ('Link Following')	25-Oct-2023	7.5	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. A website may be able to access sensitive user data when resolving symlinks. **CVE ID : CVE-2023-42844**	https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213983, https://support.apple.com/kb/HT213984, https://support.apple.com/kb/HT213985	O-APP-MACO-281123/3439
N/A	25-Oct-2023	7.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An attacker may be able to access passkeys without authentication. **CVE ID : CVE-2023-42847**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213982, https://support.apple.com/kb/HT213984	O-APP-MACO-281123/3440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Oct-2023	6.8	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data. **CVE ID : CVE-2023-41988**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213982, https://support.apple.com/kb/HT213984, https://support.apple.com/kb/HT213988	O-APP-MACO-281123/3441
N/A	25-Oct-2023	6.8	The issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1. An attacker may be able to execute arbitrary code as root from the Lock Screen. **CVE ID : CVE-2023-41989**	https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213984	O-APP-MACO-281123/3442
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-	O-APP-MACO-281123/3443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13.6.1, macOS Sonoma 14.1. Processing an image may result in disclosure of process memory. **CVE ID : CVE-2023-40416**	us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, Safari 17.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Processing web content may lead to a denial-of-service. **CVE ID : CVE-2023-41983**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213984	O-APP-MACO-281123/3444
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An attacker that has already achieved kernel code execution may be able to bypass kernel	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985	O-APP-MACO-281123/3445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory mitigations. **CVE ID : CVE-2023-42849**		
Incorrect Permission Assignment for Critical Resource	25-Oct-2023	6.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1. An attacker with knowledge of a standard user's credentials can unlock another standard user's locked screen on the same Mac. **CVE ID : CVE-2023-42861**	https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213984	O-APP-MACO-281123/3446
N/A	25-Oct-2023	5.5	The issue was addressed with improved handling of caches. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to read sensitive location information. **CVE ID : CVE-2023-40413**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985	O-APP-MACO-281123/3447
N/A	25-Oct-2023	5.5	A permissions issue was addressed with	https://support.apple.com/en-us/HT213983,	O-APP-MACO-281123/3448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional restrictions. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. An app may be able to access sensitive user data. **CVE ID : CVE-2023-40421**	https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213983, https://support.apple.com/kb/HT213984, https://support.apple.com/kb/HT213985	
N/A	25-Oct-2023	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.1. An app may be able to access user-sensitive data. **CVE ID : CVE-2023-40444**	https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213984	O-APP-MACO-281123/3449
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to cause a denial-of-service.	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support	O-APP-MACO-281123/3450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-40449	.apple.com/kb/HT213981	
N/A	25-Oct-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An app may be able to access sensitive user data. **CVE ID : CVE-2023-41072**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213982, https://support.apple.com/kb/HT213984	O-APP-MACO-281123/3451
Insertion of Sensitive Information into Log File	25-Oct-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to access sensitive user data. **CVE ID : CVE-2023-41254**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	O-APP-MACO-281123/3452
N/A	25-Oct-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.1. An app may be able to access sensitive user data.	https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213984	O-APP-MACO-281123/3453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-42842		
N/A	25-Oct-2023	5.5	The issue was addressed with improved permissions logic. This issue is fixed in macOS Sonoma 14.1. An app may be able to access sensitive user data. **CVE ID : CVE-2023-42850**	https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213984	O-APP-MACO-281123/3454
N/A	25-Oct-2023	5.5	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. An app may be able to cause a denial-of-service to Endpoint Security clients. **CVE ID : CVE-2023-42854**	https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213983, https://support.apple.com/kb/HT213984, https://support.apple.com/kb/HT213985	O-APP-MACO-281123/3455
Missing Authentication for Critical Function	25-Oct-2023	5.3	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. Photos in the Hidden Photos Album may be	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213982, https://support	O-APP-MACO-281123/3456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			viewed without authentication. **CVE ID : CVE-2023-42845**	.apple.com/kb/HT213984	
N/A	25-Oct-2023	4.6	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data. **CVE ID : CVE-2023-41982**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-MACO-281123/3457
N/A	25-Oct-2023	4.6	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data. **CVE ID : CVE-2023-41997**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-MACO-281123/3458
N/A	25-Oct-2023	4.3	This issue was addressed by	https://support.apple.com/en-	O-APP-MACO-281123/3459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removing the vulnerable code. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. A website may be able to access the microphone without the microphone use indicator being shown. **CVE ID : CVE-2023-41975**	us/HT213983, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213983, https://support.apple.com/kb/HT213984, https://support.apple.com/kb/HT213985	
N/A	25-Oct-2023	4.3	The issue was addressed with improved handling of caches. This issue is fixed in macOS Sonoma 14.1, iOS 16.7.2 and iPadOS 16.7.2. Visiting a malicious website may reveal browsing history. **CVE ID : CVE-2023-41977**	https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213984	O-APP-MACO-281123/3460
N/A	25-Oct-2023	4.3	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1. Visiting a malicious website may lead to user interface spoofing.	https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213984	O-APP-MACO-281123/3461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-42438		
Insertion of Sensitive Information into Log File	25-Oct-2023	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An app may be able to access sensitive user data. **CVE ID : CVE-2023-42857**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213982, https://support.apple.com/kb/HT213984	O-APP-MACO-281123/3462
Product: mac_os_x					
Affected Version(s): -					
N/A	20-Oct-2023	7.8	VMware Fusion(13.x prior to 13.5) contains a local privilege escalation vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges	https://www.vmware.com/security/advisories/VMSA-2023-0022.html	O-APP-MAC_-281123/3463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to root on the system where Fusion is installed or being installed for the first time. **CVE ID : CVE-2023-34045**		
Time-of-check Time-of-use (TOCTOU) Race Condition	20-Oct-2023	7	VMware Fusion(13.x prior to 13.5) contains a TOCTOU (Time-of-check Time-of-use) vulnerability that occurs during installation for the first time (the user needs to drag or copy the application to a folder from the '.dmg' volume) or when installing an upgrade. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system where Fusion is installed or being installed for the first time. **CVE ID : CVE-2023-34046**	https://www.vmware.com/security/advisories/VMSA-2023-0022.html	O-APP-MAC_-281123/3464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	20-Oct-2023	6	VMware Workstation(17.x prior to 17.5) and Fusion(13.x prior to 13.5) contain an out-of-bounds read vulnerability that exists in the functionality for sharing host Bluetooth devices with the virtual machine. A malicious actor with local administrative privileges on a virtual machine may be able to read privileged information contained in hypervisor memory from a virtual machine. **CVE ID : CVE-2023-34044**	https://www.vmware.com/security/advisories/VMSA-2023-0022.html	O-APP-MAC_-281123/3465
Product: tvos					
Affected Version(s): * Up to (excluding) 17.1					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1,	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-	O-APP-TVOS-281123/3466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tvOS 17.1. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2023-40447**	us/HT213986, https://support.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	
Use After Free	25-Oct-2023	8.8	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2023-41976**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	O-APP-TVOS-281123/3467
N/A	25-Oct-2023	8.8	A logic issue was addressed with improved checks. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution.	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support	O-APP-TVOS-281123/3468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-42852	.apple.com/en-us/HT213984	
N/A	25-Oct-2023	5.3	This issue was addressed by removing the vulnerable code. This issue is fixed in watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, tvOS 17.1, iOS 17.1 and iPadOS 17.1. A device may be passively tracked by its Wi-Fi MAC address. **CVE ID : CVE-2023-42846**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213987, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-TVOS-281123/3469
Product: watchos					
Affected Version(s): * Up to (excluding) 10.1					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2023-40447**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	O-APP-WATC-281123/3470
Use After Free	25-Oct-2023	8.8	A use-after-free issue was	https://support.apple.com/en-	O-APP-WATC-281123/3471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addressed with improved memory management. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2023-41976**	us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	
N/A	25-Oct-2023	8.8	A logic issue was addressed with improved checks. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2023-42852**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213986, https://support.apple.com/en-us/HT213987, https://support.apple.com/en-us/HT213984	O-APP-WATC-281123/3472
N/A	25-Oct-2023	6.8	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-	O-APP-WATC-281123/3473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data. **CVE ID : CVE-2023-41988**	us/HT213984, https://support.apple.com/kb/HT213982, https://support.apple.com/kb/HT213984, https://support.apple.com/kb/HT213988	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Oct-2023	6.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations. **CVE ID : CVE-2023-42849**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985	O-APP-WATC-281123/3474
N/A	25-Oct-2023	5.5	The issue was addressed with improved handling of caches. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213983, https://support.apple.com/en-us/HT213981, https://support	O-APP-WATC-281123/3475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to read sensitive location information. **CVE ID : CVE-2023-40413**	.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985	
Insertion of Sensitive Information into Log File	25-Oct-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to access sensitive user data. **CVE ID : CVE-2023-41254**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/en-us/HT213985, https://support.apple.com/kb/HT213981	O-APP-WATC-281123/3476
N/A	25-Oct-2023	5.3	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Hide My Email may be deactivated unexpectedly.	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support	O-APP-WATC-281123/3477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-40408	.apple.com/kb/HT213982	
N/A	25-Oct-2023	5.3	This issue was addressed by removing the vulnerable code. This issue is fixed in watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, tvOS 17.1, iOS 17.1 and iPadOS 17.1. A device may be passively tracked by its Wi-Fi MAC address. **CVE ID : CVE-2023-42846**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213987, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-WATC-281123/3478
N/A	25-Oct-2023	4.6	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data. **CVE ID : CVE-2023-41982**	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	O-APP-WATC-281123/3479
N/A	25-Oct-2023	4.6	This issue was addressed by restricting options offered on a locked device. This issue is	https://support.apple.com/en-us/HT213982, https://support.apple.com/en-	O-APP-WATC-281123/3480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data. **CVE ID : CVE-2023-41997**	us/HT213981, https://support.apple.com/en-us/HT213988, https://support.apple.com/en-us/HT213984, https://support.apple.com/kb/HT213981, https://support.apple.com/kb/HT213982	
Vendor: Axis					
Product: axis_os					
Affected Version(s): * Up to (excluding) 11.6.94					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	O-AXI-AXIS-281123/3481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21414		
Affected Version(s): From (including) 10.11.55 Up to (excluding) 10.12.206					
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	O-AXI-AXIS-281123/3482
Affected Version(s): From (including) 10.5.0 Up to (excluding) 10.12.199					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Oct-2023	7.2	GoSecure on behalf of Genetec Inc. has found a flaw that allows for a remote code execution during the installation of ACAP applications on the Axis device. The application handling service in	https://www.axis.com/dam/public/ad/ff/83/cve-2023-21413pdf-en-US-412755.pdf	O-AXI-AXIS-281123/3483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AXIS OS was vulnerable to command injection allowing an attacker to run arbitrary code. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21413**		
Affected Version(s): From (including) 11.0.81 Up to (excluding) 11.6.94					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Oct-2023	8.1	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API overlay_del.cgi is vulnerable to path traversal attacks that allows for file deletion. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more	https://www.axis.com/dam/public/b6/55/e2/cve-2023-21415pdf-en-US-416245.pdf	O-AXI-AXIS-281123/3484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information and solution. **CVE ID : CVE-2023-21415**		
Affected Version(s): From (including) 11.0.89 Up to (excluding) 11.6.94					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Oct-2023	7.2	GoSecure on behalf of Genetec Inc. has found a flaw that allows for a remote code execution during the installation of ACAP applications on the Axis device. The application handling service in AXIS OS was vulnerable to command injection allowing an attacker to run arbitrary code. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21413**	https://www.axis.com/dam/public/ad/ff/83/cve-2023-21413pdf-en-US-412755.pdf	O-AXI-AXIS-281123/3485
N/A	16-Oct-2023	6.8	NCC Group has found a flaw during the annual internal penetration test ordered by Axis Communications. The protection for	https://www.axis.com/dam/public/45/3c/a1/cve-2023-21414pdf-en-US-412758.pdf	O-AXI-AXIS-281123/3486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device tampering (commonly known as Secure Boot) contains a flaw which provides an opportunity for a sophisticated attack to bypass this protection. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21414**		
Affected Version(s): From (including) 6.50.5.3 Up to (excluding) 6.50.5.14					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Oct-2023	8.1	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API overlay_del.cgi is vulnerable to path traversal attacks that allows for file deletion. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer	https://www.axis.com/dam/public/b6/55/e2/cve-2023-21415pdf-en-US-416245.pdf	O-AXI-AXIS-281123/3487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21415**		
Product: axis_os_2016					
Affected Version(s): From (including) 6.50.2 Up to (excluding) 6.50.5.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Oct-2023	8.1	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API overlay_del.cgi is vulnerable to path traversal attacks that allows for file deletion. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21415**	https://www.axis.com/dam/public/b6/55/e2/cve-2023-21415pdf-en-US-416245.pdf	O-AXI-AXIS-281123/3488
Product: axis_os_2018					
Affected Version(s): * Up to (excluding) 8.40.35					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Oct-2023	8.1	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API overlay_del.cgi is vulnerable to path traversal attacks that allows for file deletion. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21415**	https://www.axis.com/dam/public/b6/55/e2/cve-2023-21415pdf-en-US-416245.pdf	O-AXI-AXIS-281123/3489
Product: axis_os_2020					
Affected Version(s): * Up to (excluding) 9.80.47					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Oct-2023	8.1	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API overlay_del.cgi is vulnerable to path traversal attacks that allows for file deletion. This flaw	https://www.axis.com/dam/public/b6/55/e2/cve-2023-21415pdf-en-US-416245.pdf	O-AXI-AXIS-281123/3490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can only be exploited after authenticating with an operator- or administrator-privileged service account. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21415**		
Product: axis_os_2022					
Affected Version(s): * Up to (excluding) 10.12.206					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Oct-2023	8.1	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API overlay_del.cgi is vulnerable to path traversal attacks that allows for file deletion. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more	https://www.axis.com/dam/public/b6/55/e2/cve-2023-21415pdf-en-US-416245.pdf	O-AXI-AXIS-281123/3491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information and solution. **CVE ID : CVE-2023-21415**		
Vendor: bakerhughes					
Product: bentley_nevada_3500_system_firmware					
Affected Version(s): 5.0.5					
Cleartext Transmission of Sensitive Information	19-Oct-2023	8.2	Baker Hughes – Bently Nevada 3500 System TDI Firmware version 5.05 contains a cleartext transmission vulnerability which could allow an attacker to steal the authentication secret from communication traffic to the device and reuse it for arbitrary requests. **CVE ID : CVE-2023-34441**	N/A	O-BAK-BENT-281123/3492
Exposure of Sensitive Information to an Unauthorized Actor	19-Oct-2023	7.5	Baker Hughes – Bently Nevada 3500 System TDI Firmware version 5.05 contains a vulnerability in their password retrieval functionality which could allow an attacker to access passwords stored on the device. **CVE ID : CVE-2023-34437**	N/A	O-BAK-BENT-281123/3493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	19-Oct-2023	6.5	Baker Hughes – Bently Nevada 3500 System TDI Firmware version 5.05 contains a replay vulnerability which could allow an attacker to replay older captured packets of traffic to the device to gain access. **CVE ID : CVE-2023-36857**	N/A	O-BAK-BENT-281123/3494
Vendor: boschrexroth					
Product: ctrlx_hmi_web_panel_wr2107_firmware					
Affected Version(s): *					
Missing Authentication for Critical Function	25-Oct-2023	8.8	The vulnerability allows an unprivileged user with access to the subnet of the TPC-110W device to gain a root shell on the device itself abusing the lack of authentication of the 'su' binary file installed on the device that can be accessed through the ADB (Android Debug Bridge) protocol exposed on the network. **CVE ID : CVE-2023-41255**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3495
Missing Authentication for	25-Oct-2023	8.8	The Android Client application, when enrolled with the	https://psirt.bosch.com/security-	O-BOS-CTRL-281123/3496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			define method 1(the user manually inserts the server ip address), use HTTP protocol to retrieve sensitive information (ip address and credentials to connect to a remote MQTT broker entity) instead of HTTPS and this feature is not configurable by the user. **CVE ID : CVE-2023-45220**	advisories/BOSCH-SA-175607.html	
Cleartext Transmission of Sensitive Information	25-Oct-2023	8.8	The Android Client application, when enrolled with the define method 1 (the user manually inserts the server ip address), use HTTP protocol to retrieve sensitive information (ip address and credentials to connect to a remote MQTT broker entity) instead of HTTPS and this feature is not configurable by the user. Due to the lack of encryption of HTTP,this issue allows an attacker placed in the same subnet network of	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the HMI device to intercept username and password necessary to authenticate to the MQTT server responsible to implement the remote management protocol. **CVE ID : CVE-2023-45321**		
Missing Authentication for Critical Function	25-Oct-2023	8.8	The Android Client application, when enrolled to the AppHub server,connects to an MQTT broker without enforcing any server authentication. This issue allows an attacker to force the Android Client application to connect to a malicious MQTT broker, enabling it to send fake messages to the HMI device **CVE ID : CVE-2023-45851**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3498
Use of Hard-coded Credentials	25-Oct-2023	8.8	The Android Client application, when enrolled to the AppHub server, connects to an MQTT broker to exchange messages and	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receive commands to execute on the HMI device. The protocol builds on top of MQTT to implement the remote management of the device is encrypted with a hard-coded DES symmetric key, that can be retrieved reversing both the Android Client application and the server-side web application. This issue allows an attacker able to control a malicious MQTT broker on the same subnet network of the device, to craft malicious messages and send them to the HMI device, executing arbitrary commands on the device itself. **CVE ID : CVE-2023-46102**		
Use of Hard-coded Credentials	25-Oct-2023	7.8	The vulnerability allows an unprivileged (untrusted) third-party application to arbitrary modify the server settings of the Android Client application,	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inducing it to connect to an attacker - controlled malicious server.This is possible by forging a valid broadcast intent encrypted with a hardcoded RSA key pair **CVE ID : CVE-2023-41372**		
Missing Authorization	25-Oct-2023	7.8	The vulnerability allows a low privileged (untrusted) application to modify a critical system property that should be denied, in order to enable the ADB (Android Debug Bridge) protocol to be exposed on the network, exploiting it to gain a privileged shell on the device without requiring the physical access through USB. **CVE ID : CVE-2023-43488**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3501
N/A	25-Oct-2023	6.8	The vulnerability allows a low privileged user that have access to the device when locked in Kiosk mode to install an arbitrary	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android application and leverage it to have access to critical device settings such as the device power management or eventually the device secure settings (ADB debug). **CVE ID : CVE-2023-45844**		
N/A	25-Oct-2023	3.3	The vulnerability allows an unprivileged(untrusted) third-party application to interact with a content-provider unsafely exposed by the Android Agent application, potentially modifying sensitive settings of the Android Client application itself. **CVE ID : CVE-2023-41960**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3503
Product: ctrlx_hmi_web_panel_wr2110_firmware					
Affected Version(s): *					
Missing Authentication for Critical Function	25-Oct-2023	8.8	The vulnerability allows an unprivileged user with access to the subnet of the TPC-110W device to gain a root shell on the device itself	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			abusing the lack of authentication of the 'su' binary file installed on the device that can be accessed through the ADB (Android Debug Bridge) protocol exposed on the network. **CVE ID : CVE-2023-41255**		
Missing Authentication for Critical Function	25-Oct-2023	8.8	The Android Client application, when enrolled with the define method 1(the user manually inserts the server ip address), use HTTP protocol to retrieve sensitive information (ip address and credentials to connect to a remote MQTT broker entity) instead of HTTPS and this feature is not configurable by the user. **CVE ID : CVE-2023-45220**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3505
Cleartext Transmission of Sensitive Information	25-Oct-2023	8.8	The Android Client application, when enrolled with the define method 1 (the user manually inserts the server ip address), use HTTP protocol to	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retrieve sensitive information (ip address and credentials to connect to a remote MQTT broker entity) instead of HTTPS and this feature is not configurable by the user. Due to the lack of encryption of HTTP,this issue allows an attacker placed in the same subnet network of the HMI device to intercept username and password necessary to authenticate to the MQTT server responsible to implement the remote management protocol. **CVE ID : CVE-2023-45321**		
Missing Authentication for Critical Function	25-Oct-2023	8.8	The Android Client application, when enrolled to the AppHub server,connects to an MQTT broker without enforcing any server authentication. This issue allows an attacker to force the Android Client application to connect to a	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious MQTT broker, enabling it to send fake messages to the HMI device **CVE ID : CVE-2023-45851**		
Use of Hard-coded Credentials	25-Oct-2023	8.8	The Android Client application, when enrolled to the AppHub server, connects to an MQTT broker to exchange messages and receive commands to execute on the HMI device. The protocol builds on top of MQTT to implement the remote management of the device is encrypted with a hard-coded DES symmetric key, that can be retrieved reversing both the Android Client application and the server-side web application. This issue allows an attacker able to control a malicious MQTT broker on the same subnet network of the device, to craft malicious messages and send them to the HMI	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device, executing arbitrary commands on the device itself. **CVE ID : CVE-2023-46102**		
Use of Hard-coded Credentials	25-Oct-2023	7.8	The vulnerability allows an unprivileged (untrusted) third-party application to arbitrary modify the server settings of the Android Client application, inducing it to connect to an attacker - controlled malicious server.This is possible by forging a valid broadcast intent encrypted with a hardcoded RSA key pair **CVE ID : CVE-2023-41372**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3509
Missing Authorization	25-Oct-2023	7.8	The vulnerability allows a low privileged (untrusted) application to modify a critical system property that should be denied, in order to enable the ADB (Android Debug Bridge) protocol to be exposed on the network, exploiting	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it to gain a privileged shell on the device without requiring the physical access through USB. **CVE ID : CVE-2023-43488**		
N/A	25-Oct-2023	6.8	The vulnerability allows a low privileged user that have access to the device when locked in Kiosk mode to install an arbitrary Android application and leverage it to have access to critical device settings such as the device power management or eventually the device secure settings (ADB debug). **CVE ID : CVE-2023-45844**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3511
N/A	25-Oct-2023	3.3	The vulnerability allows an unprivileged(untrusted) third-party application to interact with a content-provider unsafely exposed by the Android Agent application, potentially modifying sensitive settings of the	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android Client application itself. **CVE ID : CVE-2023-41960**		
Product: ctrlx_hmi_web_panel_wr2115_firmware					
Affected Version(s): *					
Missing Authentication for Critical Function	25-Oct-2023	8.8	The vulnerability allows an unprivileged user with access to the subnet of the TPC-110W device to gain a root shell on the device itself abusing the lack of authentication of the 'su' binary file installed on the device that can be accessed through the ADB (Android Debug Bridge) protocol exposed on the network. **CVE ID : CVE-2023-41255**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3513
Missing Authentication for Critical Function	25-Oct-2023	8.8	The Android Client application, when enrolled with the define method 1(the user manually inserts the server ip address), use HTTP protocol to retrieve sensitive information (ip address and credentials to connect to a remote MQTT broker entity)	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			instead of HTTPS and this feature is not configurable by the user. **CVE ID : CVE-2023-45220**		
Cleartext Transmission of Sensitive Information	25-Oct-2023	8.8	The Android Client application, when enrolled with the define method 1 (the user manually inserts the server ip address), use HTTP protocol to retrieve sensitive information (ip address and credentials to connect to a remote MQTT broker entity) instead of HTTPS and this feature is not configurable by the user. Due to the lack of encryption of HTTP,this issue allows an attacker placed in the same subnet network of the HMI device to intercept username and password necessary to authenticate to the MQTT server responsible to implement the remote management protocol. **CVE ID : CVE-2023-45321**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	25-Oct-2023	8.8	The Android Client application, when enrolled to the AppHub server,connects to an MQTT broker without enforcing any server authentication. This issue allows an attacker to force the Android Client application to connect to a malicious MQTT broker, enabling it to send fake messages to the HMI device **CVE ID : CVE-2023-45851**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3516
Use of Hard-coded Credentials	25-Oct-2023	8.8	The Android Client application, when enrolled to the AppHub server, connects to an MQTT broker to exchange messages and receive commands to execute on the HMI device. The protocol builds on top of MQTT to implement the remote management of the device is encrypted with a hard-coded DES symmetric key, that can be retrieved reversing	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			both the Android Client application and the server-side web application. This issue allows an attacker able to control a malicious MQTT broker on the same subnet network of the device, to craft malicious messages and send them to the HMI device, executing arbitrary commands on the device itself. **CVE ID : CVE-2023-46102**		
Use of Hard-coded Credentials	25-Oct-2023	7.8	The vulnerability allows an unprivileged (untrusted) third-party application to arbitrary modify the server settings of the Android Client application, inducing it to connect to an attacker - controlled malicious server.This is possible by forging a valid broadcast intent encrypted with a hardcoded RSA key pair **CVE ID : CVE-2023-41372**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	25-Oct-2023	7.8	The vulnerability allows a low privileged (untrusted) application to modify a critical system property that should be denied, in order to enable the ADB (Android Debug Bridge) protocol to be exposed on the network, exploiting it to gain a privileged shell on the device without requiring the physical access through USB. **CVE ID : CVE-2023-43488**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3519
N/A	25-Oct-2023	6.8	The vulnerability allows a low privileged user that have access to the device when locked in Kiosk mode to install an arbitrary Android application and leverage it to have access to critical device settings such as the device power management or eventually the device secure settings (ADB debug).	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45844		
N/A	25-Oct-2023	3.3	The vulnerability allows an unprivileged(untrusted) third-party application to interact with a content-provider unsafely exposed by the Android Agent application, potentially modifying sensitive settings of the Android Client application itself. **CVE ID : CVE-2023-41960**	https://psirt.bosch.com/security-advisories/BOSCH-SA-175607.html	O-BOS-CTRL-281123/3521
Vendor: byzoro					
Product: smart_s85f_firmware					
Affected Version(s): * Up to (including) 2023-10-10					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-2023	9.8	A vulnerability was found in Beijing Baichuo Smart S85F Management Platform up to 20231010 and classified as critical. This issue affects some unknown processing of the file /sysmanage/importconf.php. The manipulation of the argument btn_file_renew leads to os command injection. The	N/A	O-BYZ-SMAR-281123/3522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-243059. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-5683**		
Affected Version(s): * Up to (including) 2023-10-12					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-2023	9.8	A vulnerability was found in Beijing Baichuo Smart S85F Management Platform up to 20231012. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /importexport.php. The manipulation leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-	N/A	O-BYZ-SMAR-281123/3523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			243061 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-5684**		
Vendor: Cisco					
Product: ios_xe					
Affected Version(s): * Up to (excluding) 17.9.4a					
N/A	16-Oct-2023	10	Cisco is providing an update for the ongoing investigation into observed exploitation of the web UI feature in Cisco IOS XE Software. We are updating the list of fixed releases and adding the Software Checker. Our investigation has determined that the actors exploited two previously unknown issues. The attacker first exploited CVE-2023-20198 to gain initial access and issued a privilege 15 command to create a local user and password	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	O-CIS-IOS_-281123/3524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			combination. This allowed the user to log in with normal user access. The attacker then exploited another component of the web UI feature, leveraging the new local user to elevate privilege to root and write the implant to the file system. Cisco has assigned CVE-2023-20273 to this issue. CVE-2023-20198 has been assigned a CVSS Score of 10.0. CVE-2023-20273 has been assigned a CVSS Score of 7.2. Both of these CVEs are being tracked by CSCwh87343. **CVE ID : CVE-2023-20198**		
Affected Version(s): From (including) 16.12 Up to (excluding) 16.12.10a					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	O-CIS-IOS_-281123/3525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Affected Version(s): From (including) 17.3 Up to (excluding) 17.3.8a					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	O-CIS-IOS_-281123/3526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20273		
Affected Version(s): From (including) 17.6 Up to (excluding) 17.6.6a					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	O-CIS-IOS_-281123/3527
Affected Version(s): From (including) 17.9 Up to (excluding) 17.9.4a					
N/A	25-Oct-2023	7.2	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z	O-CIS-IOS_-281123/3528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges. **CVE ID : CVE-2023-20273**		
Vendor: contec					
Product: solarview_compact_firmware					
Affected Version(s): * Up to (including) 6.0					
N/A	27-Oct-2023	9.8	An issue in Contec SolarView Compact v.6.0 and before allows an attacker to execute arbitrary code via the texteditor.php component. **CVE ID : CVE-2023-46509**	N/A	O-CON-SOLA-281123/3529
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
N/A	25-Oct-2023	9.8	In buc Traceroute 2.0.12 through 2.1.2 before 2.1.3, the wrapper scripts do not	N/A	O-DEB-DEBI-281123/3530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			properly parse command lines. **CVE ID : CVE-2023-46316**		
Out-of-bounds Write	25-Oct-2023	9.8	Memory safety bugs present in Firefox 118, Firefox ESR 115.3, and Thunderbird 115.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5730**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/	O-DEB-DEBI-281123/3531
Improper Verification of Cryptographic Signature	27-Oct-2023	7.5	VMware Tools contains a SAML token signature bypass vulnerability. A malicious actor that has been granted Guest Operation Privileges https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-6A952214-0E5E-4CCF-9D2A-	https://www.vmware.com/security/advisories/VMSA-2023-0024.html, http://www.openwall.com/lists/oss-security/2023/10/27/1	O-DEB-DEBI-281123/3532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			90948FF643EC.html in a target virtual machine may be able to elevate their privileges if that target virtual machine has been assigned a more privileged Guest Alias https://vdc-download.vmware.com/vmwb-repository/dcr-public/d1902b0e-d479-46bf-8ac9-cee0e31e8ec0/07ce8dbd-db48-4261-9b8f-c6d3ad8ba472/vim.vm.guest.AliasManager.html . **CVE ID : CVE-2023-34058**		
N/A	25-Oct-2023	7.5	Drivers are not always robust to extremely large draw calls and in some cases this scenario could have led to a crash. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5724**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1836705	O-DEB-DEBI-281123/3533
N/A	25-Oct-2023	7.5	During garbage collection extra operations were	https://www.mozilla.org/security/advisories/	O-DEB-DEBI-281123/3534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performed on a object that should not be. This could have led to a potentially exploitable crash. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5728**	mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1852729	
N/A	27-Oct-2023	7	open-vm-tools contains a file descriptor hijack vulnerability in the vmware-user-suid-wrapper. A malicious actor with non-root privileges may be able to hijack the /dev/uinput file descriptor allowing them to simulate user inputs. **CVE ID : CVE-2023-34059**	http://www.openwall.com/lists/oss-security/2023/10/27/2	O-DEB-DEBI-281123/3535
N/A	25-Oct-2023	6.5	An attacker could have created a malicious link using bidirectional characters to spoof the location in the address bar when visited. This vulnerability affects Firefox < 117, Firefox ESR < 115.4, and	https://www.mozilla.org/security/advisories/mfsa2023-34/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/,	O-DEB-DEBI-281123/3536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 115.4.1. **CVE ID : CVE-2023-5732**	https://bugzilla.mozilla.org/show_bug.cgi?id=1690979	
Improper Restriction of Rendered UI Layers or Frames	25-Oct-2023	4.3	It was possible for certain browser prompts and dialogs to be activated or dismissed unintentionally by the user due to an insufficient activation-delay. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5721**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1830820	O-DEB-DEBI-281123/3537
N/A	25-Oct-2023	4.3	A malicious installed WebExtension could open arbitrary URLs, which under the right circumstance could be leveraged to collect sensitive user data. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5725**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://bugzilla.mozilla.org/show_bug.cgi?id=1845739, https://www.mozilla.org/security/advisories/mfsa2023-46/	O-DEB-DEBI-281123/3538
Exposure of	18-Oct-2023	3.6	Redis is an in-memory database	https://github.com/redis/redis	O-DEB-DEBI-281123/3539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			that persists on disk. On startup, Redis begins listening on a Unix socket before adjusting its permissions to the user-provided configuration. If a permissive umask(2) is used, this creates a race condition that enables, during a short period of time, another process to establish an otherwise unauthorized connection. This problem has existed since Redis 2.6.0-RC1. This issue has been addressed in Redis versions 7.2.2, 7.0.14 and 6.2.14. Users are advised to upgrade. For users unable to upgrade, it is possible to work around the problem by disabling Unix sockets, starting Redis with a restrictive umask, or storing the Unix socket file in a protected directory.	/commit/03345ddc7faf7af079485f2cbe5d17a1611cbce1, https://github.com/redis/redis/security/advisories/GHSA-ghmp-889m-7cvx	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45145		
Affected Version(s): 11.0					
N/A	25-Oct-2023	9.8	In buc Traceroute 2.0.12 through 2.1.2 before 2.1.3, the wrapper scripts do not properly parse command lines. **CVE ID : CVE-2023-46316**	N/A	O-DEB-DEBI-281123/3540
Out-of-bounds Write	25-Oct-2023	9.8	Memory safety bugs present in Firefox 118, Firefox ESR 115.3, and Thunderbird 115.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5730**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/	O-DEB-DEBI-281123/3541
Use After Free	25-Oct-2023	8.8	Use after free in Profiles in Google Chrome prior to 118.0.5993.117 allowed a remote attacker to potentially exploit heap corruption	https://chromereleases.googleblog.com/2023/10/stable-channel-update-for-desktop_24.html	O-DEB-DEBI-281123/3542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-5472**		
Out-of-bounds Write	25-Oct-2023	7.8	A out-of-bounds write flaw was found in the xorg-x11-server. This issue occurs due to an incorrect calculation of a buffer offset when copying data stored in the heap in the XIChangeDeviceProperty function in Xi/xiproperty.c and in RRChangeOutputProperty function in randr/rrproperty.c, allowing for possible escalation of privileges or denial of service. **CVE ID : CVE-2023-5367**	https://lists.x.org/archives/xorg-announce/2023-October/003430.html	O-DEB-DEBI-281123/3543
Improper Verification of Cryptographic Signature	27-Oct-2023	7.5	VMware Tools contains a SAML token signature bypass vulnerability. A malicious actor that has been granted Guest Operation Privileges https://docs.vmware.com/en/VMware-	https://www.vmware.com/security/advisories/VMSA-2023-0024.html, http://www.openwall.com/lists/oss-security/2023/10/27/1	O-DEB-DEBI-281123/3544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vSphere/8.0/vsphere-security/GUID-6A952214-0E5E-4CCF-9D2A-90948FF643EC.html in a target virtual machine may be able to elevate their privileges if that target virtual machine has been assigned a more privileged Guest Alias https://vdc-download.vmware.com/vmwb-repository/dcr-public/d1902b0e-d479-46bf-8ac9-cee0e31e8ec0/07ce8dbd-db48-4261-9b8f-c6d3ad8ba472/vim.vm.guest.AliasManager.html . **CVE ID : CVE-2023-34058**		
Improper Verification of Cryptographic Signature	26-Oct-2023	7.5	browserify-sign is a package to duplicate the functionality of node's crypto public key functions, much of this is based on Fedor Indutny's work on indutny/tls.js. An upper bound check issue in `dsaVerify` function allows an attacker to	N/A	O-DEB-DEBI-281123/3545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			construct signatures that can be successfully verified by any public key, thus leading to a signature forgery attack. All places in this project that involve DSA verification of user-input signatures will be affected by this vulnerability. This issue has been patched in version 4.2.2. **CVE ID : CVE-2023-46234**		
N/A	25-Oct-2023	7.5	Drivers are not always robust to extremely large draw calls and in some cases this scenario could have led to a crash. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5724**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1836705	O-DEB-DEBI-281123/3546
N/A	25-Oct-2023	7.5	During garbage collection extra operations were performed on a object that should not be. This could have led to a	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/	O-DEB-DEBI-281123/3547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially exploitable crash. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5728**	mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1852729	
N/A	27-Oct-2023	7	open-vm-tools contains a file descriptor hijack vulnerability in the vmware-user-suid-wrapper. A malicious actor with non-root privileges may be able to hijack the /dev/uinput file descriptor allowing them to simulate user inputs. **CVE ID : CVE-2023-34059**	http://www.openwall.com/lists/oss-security/2023/10/27/2	O-DEB-DEBI-281123/3548
N/A	25-Oct-2023	6.5	An attacker could have created a malicious link using bidirectional characters to spoof the location in the address bar when visited. This vulnerability affects Firefox < 117, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5732**	https://www.mozilla.org/security/advisories/mfsa2023-34/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1690979	O-DEB-DEBI-281123/3549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	5.4	Roundcube before 1.4.15, 1.5.x before 1.5.5, and 1.6.x before 1.6.4 allows stored XSS via an HTML e-mail message with a crafted SVG document because of program/lib/Roundcube/rcube_washtml.php behavior. This could allow a remote attacker to load arbitrary JavaScript code. **CVE ID : CVE-2023-5631**	https://github.com/roundcube/roundcubemail/commit/6ee6e7ae301e165e2b2cb703edf75552e5376613, https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1054079, https://github.com/roundcube/roundcubemail/commit/41756cc3331b495cc0b71886984474dc529dd31d	O-DEB-DEBI-281123/3550
Use After Free	25-Oct-2023	4.7	A use-after-free flaw was found in the xorg-x11-server. An X server crash may occur in a very specific and legacy configuration (a multi-screen setup with multiple protocol screens, also known as Zaphod mode) if the pointer is warped from within a window on one screen to the root window of the other screen and if the original window is	https://lists.x.org/archives/xorg-announce/2023-October/003430.html	O-DEB-DEBI-281123/3551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			destroyed followed by another window being destroyed. **CVE ID : CVE-2023-5380**		
Improper Restriction of Rendered UI Layers or Frames	25-Oct-2023	4.3	It was possible for certain browser prompts and dialogs to be activated or dismissed unintentionally by the user due to an insufficient activation-delay. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5721**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/security/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1830820	O-DEB-DEBI-281123/3552
N/A	25-Oct-2023	4.3	A malicious installed WebExtension could open arbitrary URLs, which under the right circumstance could be leveraged to collect sensitive user data. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5725**	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://bugzilla.mozilla.org/show_bug.cgi?id=1845739, https://www.mozilla.org/security/advisories/mfsa2023-46/	O-DEB-DEBI-281123/3553
Affected Version(s): 12.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Oct-2023	9.8	In buc Traceroute 2.0.12 through 2.1.2 before 2.1.3, the wrapper scripts do not properly parse command lines. **CVE ID : CVE-2023-46316**	N/A	O-DEB-DEBI-281123/3554
Use After Free	25-Oct-2023	8.8	Use after free in Profiles in Google Chrome prior to 118.0.5993.117 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-5472**	https://chromereleases.googleblog.com/2023/10/stable-channel-update-for-desktop_24.html	O-DEB-DEBI-281123/3555
Out-of-bounds Write	25-Oct-2023	7.8	A out-of-bounds write flaw was found in the xorg-x11-server. This issue occurs due to an incorrect calculation of a buffer offset when copying data stored in the heap in the XIChangeDeviceProperty function in Xi/xiproperty.c and in RRChangeOutputProperty function in randr/rrproperty.c, allowing for possible escalation	https://lists.x.org/archives/xorg-announce/2023-October/003430.html	O-DEB-DEBI-281123/3556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privileges or denial of service. **CVE ID : CVE-2023-5367**		
Improper Verification of Cryptographic Signature	27-Oct-2023	7.5	VMware Tools contains a SAML token signature bypass vulnerability. A malicious actor that has been granted Guest Operation Privileges https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-6A952214-0E5E-4CCF-9D2A-90948FF643EC.html in a target virtual machine may be able to elevate their privileges if that target virtual machine has been assigned a more privileged Guest Alias https://vdc-download.vmware.com/vmwb-repository/dcr-public/d1902b0e-d479-46bf-8ac9-cee0e31e8ec0/07ce8dbd-db48-4261-9b8f-c6d3ad8ba472/vim.vm.guest.AliasManager.html .	https://www.vmware.com/security/advisories/VMSA-2023-0024.html, http://www.openwall.com/lists/oss-security/2023/10/27/1	O-DEB-DEBI-281123/3557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34058		
Improper Verification of Cryptographic Signature	26-Oct-2023	7.5	browserify-sign is a package to duplicate the functionality of node's crypto public key functions, much of this is based on Fedor Indutny's work on indutny/tls.js. An upper bound check issue in `dsaVerify` function allows an attacker to construct signatures that can be successfully verified by any public key, thus leading to a signature forgery attack. All places in this project that involve DSA verification of user-input signatures will be affected by this vulnerability. This issue has been patched in version 4.2.2. **CVE ID : CVE-2023-46234**	N/A	O-DEB-DEBI-281123/3558
N/A	27-Oct-2023	7	open-vm-tools contains a file descriptor hijack vulnerability in the vmware-user-suid-wrapper. A	http://www.openwall.com/lists/oss-security/2023/10/27/2	O-DEB-DEBI-281123/3559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious actor with non-root privileges may be able to hijack the /dev/uinput file descriptor allowing them to simulate user inputs. **CVE ID : CVE-2023-34059**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-2023	5.4	Roundcube before 1.4.15, 1.5.x before 1.5.5, and 1.6.x before 1.6.4 allows stored XSS via an HTML e-mail message with a crafted SVG document because of program/lib/Roundcube/rcube_washtml.php behavior. This could allow a remote attacker to load arbitrary JavaScript code. **CVE ID : CVE-2023-5631**	https://github.com/roundcube/roundcubemail/commit/6ee6e7ae301e165e2b2cb703edf75552e5376613, https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1054079, https://github.com/roundcube/roundcubemail/commit/41756cc3331b495cc0b71886984474dc529dd31d	O-DEB-DEBI-281123/3560
Use After Free	25-Oct-2023	4.7	A use-after-free flaw was found in the xorg-x11-server. An X server crash may occur in a very specific and legacy configuration (a multi-screen setup with multiple	https://lists.x.org/archives/xorg-announce/2023-October/003430.html	O-DEB-DEBI-281123/3561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocol screens, also known as Zaphod mode) if the pointer is warped from within a window on one screen to the root window of the other screen and if the original window is destroyed followed by another window being destroyed. **CVE ID : CVE-2023-5380**		
Vendor: Dlink					
Product: dar-7000_firmware					
Affected Version(s): 31r02b1413c					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-2023	9.8	SQL injection vulnerability in D-Link Online behavior audit gateway DAR-7000 V31R02B1413C allows a remote attacker to obtain sensitive information and execute arbitrary code via the editrole.php component. **CVE ID : CVE-2023-42406**	N/A	O-DLI-DAR--281123/3562
Affected Version(s): v31r02b1413c					
Improper Neutralization of Special Elements	17-Oct-2023	9.8	D-Link Online behavior audit gateway DAR-7000 V31R02B1413C is vulnerable to SQL	N/A	O-DLI-DAR--281123/3563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			Injection via /importexport.php. **CVE ID : CVE-2023-44693**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Oct-2023	9.8	D-Link Online behavior audit gateway DAR-7000 V31R02B1413C is vulnerable to SQL Injection via /log/mailrecvview.php. **CVE ID : CVE-2023-44694**	N/A	O-DLI-DAR--281123/3564
Product: di-7003g_firmware					
Affected Version(s): * Up to (including) 23.08.25d1					
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn	N/A	O-DLI-DI-7-281123/3565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter of the tgfile.htm function. **CVE ID : CVE-2023-45572**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the n parameter of the mrclfile_del.asp function. **CVE ID : CVE-2023-45573**	N/A	O-DLI-DI-7-281123/3566
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-	https://www.dlink.com/en/security-bulletin/	O-DLI-DI-7-281123/3567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the file.data function. **CVE ID : CVE-2023-45574**		
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to	N/A	O-DLI-DI-7-281123/3568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code via the ip parameter of the ip_position.asp function. **CVE ID : CVE-2023-45575**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the remove_ext_proto/ remove_ext_port parameter of the upnp_ctrl.asp function. **CVE ID : CVE-2023-45576**	N/A	O-DLI-DI-7-281123/3569
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1	N/A	O-DLI-DI-7-281123/3570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wanid parameter of the H5/speedlimit.data function. **CVE ID : CVE-2023-45577**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-	N/A	O-DLI-DI-7-281123/3571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the pap_en/chap_en parameter of the pppoe_base.asp function. **CVE ID : CVE-2023-45578**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip/type parameter of the jingx.asp function.	N/A	O-DLI-DI-7-281123/3572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45579		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wild/mx and other parameters of the ddns.asp function **CVE ID : CVE-2023-45580**	N/A	O-DLI-DI-7-281123/3573
Product: di-7100g\+_firmware					
Affected Version(s): * Up to (including) 23.08.23d1					
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and	N/A	O-DLI-DI-7-281123/3574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the tgfile.htm function. **CVE ID : CVE-2023-45572**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a	N/A	O-DLI-DI-7-281123/3575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code via the n parameter of the mrclfile_del.asp function. **CVE ID : CVE-2023-45573**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the file.data function. **CVE ID : CVE-2023-45574**	https://www.dlink.com/en/security-bulletin/	O-DLI-DI-7-281123/3576
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-	N/A	O-DLI-DI-7-281123/3577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip parameter of the ip_position.asp function. **CVE ID : CVE-2023-45575**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and	N/A	O-DLI-DI-7-281123/3578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the remove_ext_proto/ remove_ext_port parameter of the upnp_ctrl.asp function. **CVE ID : CVE-2023-45576**		
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wanid parameter of the H5/speedlimit.data function. **CVE ID : CVE-2023-45577**	N/A	O-DLI-DI-7-281123/3579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the pap_en/chap_en parameter of the pppoe_base.asp function. **CVE ID : CVE-2023-45578**	N/A	O-DLI-DI-7-281123/3580
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1	N/A	O-DLI-DI-7-281123/3581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip/type parameter of the jingx.asp function. **CVE ID : CVE-2023-45579**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the	N/A	O-DLI-DI-7-281123/3582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wild/mx and other parameters of the ddns.asp function **CVE ID : CVE-2023-45580**		
Product: di-7100g_firmware					
Affected Version(s): * Up to (including) 23.08.23d1					
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the tgfile.htm function. **CVE ID : CVE-2023-45572**	N/A	O-DLI-DI-7-281123/3583
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-	N/A	O-DLI-DI-7-281123/3584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the n parameter of the mrclfile_del.asp function. **CVE ID : CVE-2023-45573**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and	https://www.dlink.com/en/security-bulletin/	O-DLI-DI-7-281123/3585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the file.data function. **CVE ID : CVE-2023-45574**		
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip parameter of the ip_position.asp function. **CVE ID : CVE-2023-45575**	N/A	O-DLI-DI-7-281123/3586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the remove_ext_proto/ remove_ext_port parameter of the upnp_ctrl.asp function. **CVE ID : CVE-2023-45576**	N/A	O-DLI-DI-7-281123/3587
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-	N/A	O-DLI-DI-7-281123/3588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wanid parameter of the H5/speedlimit.data function. **CVE ID : CVE-2023-45577**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary	N/A	O-DLI-DI-7-281123/3589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code via the pap_en/chap_en parameter of the pppoe_base.asp function. **CVE ID : CVE-2023-45578**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip/type parameter of the jingx.asp function. **CVE ID : CVE-2023-45579**	N/A	O-DLI-DI-7-281123/3590
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-	N/A	O-DLI-DI-7-281123/3591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wild/mx and other parameters of the ddns.asp function **CVE ID : CVE-2023-45580**		
Product: di-7200g\+_firmware					
Affected Version(s): * Up to (including) 23.08.23d1					
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-	N/A	O-DLI-DI-7-281123/3592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the tgfile.htm function. **CVE ID : CVE-2023-45572**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the n parameter of the mrclfile_del.asp function. **CVE ID : CVE-2023-45573**	N/A	O-DLI-DI-7-281123/3593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the file.data function. **CVE ID : CVE-2023-45574**	https://www.dlink.com/en/security-bulletin/	O-DLI-DI-7-281123/3594
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-	N/A	O-DLI-DI-7-281123/3595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip parameter of the ip_position.asp function. **CVE ID : CVE-2023-45575**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the remove_ext_proto/ remove_ext_port	N/A	O-DLI-DI-7-281123/3596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter of the upnp_ctrl.asp function. **CVE ID : CVE-2023-45576**		
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wanid parameter of the H5/speedlimit.data function. **CVE ID : CVE-2023-45577**	N/A	O-DLI-DI-7-281123/3597
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and	N/A	O-DLI-DI-7-281123/3598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the pap_en/chap_en parameter of the pppoe_base.asp function. **CVE ID : CVE-2023-45578**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1	N/A	O-DLI-DI-7-281123/3599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip/type parameter of the jingx.asp function. **CVE ID : CVE-2023-45579**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wild/mx and other parameters of the ddns.asp function **CVE ID : CVE-2023-45580**	N/A	O-DLI-DI-7-281123/3600
Product: di-7200g_firmware					
Affected Version(s): * Up to (including) 23.08.23e1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the tgfile.htm function. **CVE ID : CVE-2023-45572**	N/A	O-DLI-DI-7-281123/3601
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-	N/A	O-DLI-DI-7-281123/3602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the n parameter of the mrclfile_del.asp function. **CVE ID : CVE-2023-45573**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the file.data function.	https://www.dlink.com/en/security-bulletin/	O-DLI-DI-7-281123/3603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45574		
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip parameter of the ip_position.asp function. **CVE ID : CVE-2023-45575**	N/A	O-DLI-DI-7-281123/3604
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-	N/A	O-DLI-DI-7-281123/3605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the remove_ext_proto/ remove_ext_port parameter of the upnp_ctrl.asp function. **CVE ID : CVE-2023-45576**		
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a	N/A	O-DLI-DI-7-281123/3606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code via the wanid parameter of the H5/speedlimit.data function. **CVE ID : CVE-2023-45577**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the pap_en/chap_en parameter of the pppoe_base.asp function. **CVE ID : CVE-2023-45578**	N/A	O-DLI-DI-7-281123/3607
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1	N/A	O-DLI-DI-7-281123/3608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip/type parameter of the jingx.asp function. **CVE ID : CVE-2023-45579**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-	N/A	O-DLI-DI-7-281123/3609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wild/mx and other parameters of the ddns.asp function **CVE ID : CVE-2023-45580**		
Product: di-7300g\+_firmware					
Affected Version(s): * Up to (including) 23.08.23d1					
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the tgfile.htm function.	N/A	O-DLI-DI-7-281123/3610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45572		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the n parameter of the mrclfile_del.asp function. **CVE ID : CVE-2023-45573**	N/A	O-DLI-DI-7-281123/3611
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-	https://www.dlink.com/en/security-bulletin/	O-DLI-DI-7-281123/3612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the file.data function. **CVE ID : CVE-2023-45574**		
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip	N/A	O-DLI-DI-7-281123/3613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter of the ip_position.asp function. **CVE ID : CVE-2023-45575**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the remove_ext_proto/ remove_ext_port parameter of the upnp_ctrl.asp function. **CVE ID : CVE-2023-45576**	N/A	O-DLI-DI-7-281123/3614
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-	N/A	O-DLI-DI-7-281123/3615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wanid parameter of the H5/speedlimit.data function. **CVE ID : CVE-2023-45577**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and	N/A	O-DLI-DI-7-281123/3616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the pap_en/chap_en parameter of the pppoe_base.asp function. **CVE ID : CVE-2023-45578**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip/type parameter of the jingx.asp function. **CVE ID : CVE-2023-45579**	N/A	O-DLI-DI-7-281123/3617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wild/mx and other parameters of the ddns.asp function **CVE ID : CVE-2023-45580**	N/A	O-DLI-DI-7-281123/3618
Product: di-7400g\+_firmware					
Affected Version(s): * Up to (including) 23.08.23d1					
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-	N/A	O-DLI-DI-7-281123/3619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the tgfile.htm function. **CVE ID : CVE-2023-45572**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the n	N/A	O-DLI-DI-7-281123/3620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter of the mrclfile_del.asp function. **CVE ID : CVE-2023-45573**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the fn parameter of the file.data function. **CVE ID : CVE-2023-45574**	https://www.dlink.com/en/security-bulletin/	O-DLI-DI-7-281123/3621
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-	N/A	O-DLI-DI-7-281123/3622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip parameter of the ip_position.asp function. **CVE ID : CVE-2023-45575**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a	N/A	O-DLI-DI-7-281123/3623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code via the remove_ext_proto/ remove_ext_port parameter of the upnp_ctrl.asp function. **CVE ID : CVE-2023-45576**		
Out-of-bounds Write	16-Oct-2023	9.8	Stack Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the wanid parameter of the H5/speedlimit.data function. **CVE ID : CVE-2023-45577**	N/A	O-DLI-DI-7-281123/3624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the pap_en/chap_en parameter of the pppoe_base.asp function. **CVE ID : CVE-2023-45578**	N/A	O-DLI-DI-7-281123/3625
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1	N/A	O-DLI-DI-7-281123/3626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the ip/type parameter of the jingx.asp function. **CVE ID : CVE-2023-45579**		
Out-of-bounds Write	16-Oct-2023	9.8	Buffer Overflow vulnerability in D-Link device DI-7003GV2.D1 v.23.08.25D1 and before, DI-7100G+V2.D1 v.23.08.23D1 and before, DI-7100GV2.D1 v.23.08.23D1, DI-7200G+V2.D1 v.23.08.23D1 and before, DI-7200GV2.E1 v.23.08.23E1 and before, DI-7300G+V2.D1 v.23.08.23D1, and DI-7400G+V2.D1 v.23.08.23D1 and before allows a remote attacker to execute arbitrary code via the	N/A	O-DLI-DI-7-281123/3627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wild/mx and other parameters of the ddns.asp function **CVE ID : CVE-2023-45580**		
Product: dir-820l_firmware					
Affected Version(s): 1.05b03					
Out-of-bounds Write	16-Oct-2023	9.8	D-Link DIR-820L 1.05B03 has a stack overflow vulnerability in the sub_4507CC function. **CVE ID : CVE-2023-44808**	N/A	O-DLI-DIR--281123/3628
N/A	16-Oct-2023	9.8	D-Link device DIR-820L 1.05B03 is vulnerable to Insecure Permissions. **CVE ID : CVE-2023-44809**	N/A	O-DLI-DIR--281123/3629
Product: dsl-2730u_firmware					
Affected Version(s): -					
N/A	19-Oct-2023	6.8	D-Link (Non-US) DSL-2750U N300 ADSL2+ and (Non-US) DSL-2730U N150 ADSL2+ are vulnerable to Incorrect Access Control. The UART/Serial interface on the PCB, provides log output and a root terminal without proper access control.	N/A	O-DLI-DSL--281123/3630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46033		
Product: dsl-2750u_firmware					
Affected Version(s): -					
N/A	19-Oct-2023	6.8	D-Link (Non-US) DSL-2750U N300 ADSL2+ and (Non-US) DSL-2730U N150 ADSL2+ are vulnerable to Incorrect Access Control. The UART/Serial interface on the PCB, provides log output and a root terminal without proper access control. **CVE ID : CVE-2023-46033**	N/A	O-DLI-DSL--281123/3631
Vendor: Eaton					
Product: easy-box-e4-ac1_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-EASY-281123/3632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**		
Product: easy-box-e4-dc1_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-EASY-281123/3633
Product: easy-box-e4-uc1_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-EASY-281123/3634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**		
Product: easy-e4-ac-12rc1p_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-EASY-281123/3635
Product: easy-e4-ac-12rcx1p_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-	O-EAT-EASY-281123/3636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	va-2023-1010.pdf	
Product: easy-e4-ac-16re1p_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-EASY-281123/3637
Product: easy-e4-dc-12tc1p_firmware					
Affected Version(s): * Up to (excluding) 2.02					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-EASY-281123/3638
Product: easy-e4-dc-12tcx1p_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending).	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-EASY-281123/3639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43776		
Product: easy-e4-dc-16te1p_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-EASY-281123/3640
Product: easy-e4-dc-4pe1p_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-EASY-281123/3641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**		
Product: easy-e4-dc-6ae1p_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-EASY-281123/3642
Product: easy-e4-dc-8te1p_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-EASY-281123/3643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**		
Product: easy-e4-uc-12rc1p_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-EASY-281123/3644
Product: easy-e4-uc-12rcx1p_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to	https://www.eaton.com/content/dam/eaton/company/news-insights/cybers	O-EAT-EASY-281123/3645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	ecurity/security-bulletins/etn-va-2023-1010.pdf	
Product: easy-e4-uc-16re1p_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-EASY-281123/3646
Product: easy-e4-uc-16re1_firmware					
Affected Version(s): * Up to (excluding) 2.02					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-EASY-281123/3647
Product: easy-e4-uc-8re1p_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending).	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-EASY-281123/3648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43776		
Product: easy_e4-ac-8re1p_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-EASY-281123/3649
Product: xv-102-a035tqrb-1e4_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-XV-1-281123/3650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**		
Product: xv-102-a3-57tvrb-1e4_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-XV-1-281123/3651
Product: xv100-box-e4-dc1_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-XV10-281123/3652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**		
Product: xv100-box-e4-uc1_firmware					
Affected Version(s): * Up to (excluding) 2.02					
Inadequate Encryption Strength	17-Oct-2023	6.6	Eaton easyE4 PLC offers a device password protection functionality to facilitate a secure connection and prevent unauthorized access. It was observed that the device password was stored with a weak encoding algorithm in the easyE4 program file when exported to SD card (*.PRG file ending). **CVE ID : CVE-2023-43776**	https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/etn-va-2023-1010.pdf	O-EAT-XV10-281123/3653
Vendor: Extremenetworks					
Product: exos					
Affected Version(s): * Up to (excluding) 22.7					
Incorrect Authorization	16-Oct-2023	9.8	An Access Control issue discovered in Extreme Networks Switch Engine	https://extreme-networks.my.site.com/ExtrArtic	O-EXT-EXOS-281123/3654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EXOS) before 32.5.1.5, also fixed in 22.7, 31.7.2 allows attackers to gain escalated privileges using crafted telnet commands via Redis server. **CVE ID : CVE-2023-43119**	leDetail?an=000114378	
N/A	16-Oct-2023	8.8	An issue discovered in Extreme Networks Switch Engine (EXOS) before 32.5.1.5, before 22.7 and before 31.7.1 allows attackers to gain escalated privileges via crafted HTTP request. **CVE ID : CVE-2023-43120**	https://extreme-networks.my.site.com/ExtrArticleDetail?an=000114377	O-EXT-EXOS-281123/3655
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Oct-2023	7.5	A Directory Traversal vulnerability discovered in Chalet application in Extreme Networks Switch Engine (EXOS) before 32.5.1.5, before 22.7, and before 31.7.2 allows attackers to read arbitrary files. **CVE ID : CVE-2023-43121**	https://extreme-networks.my.site.com/ExtrArticleDetail?an=000114376	O-EXT-EXOS-281123/3656
Affected Version(s): From (including) 31.0 Up to (excluding) 31.7.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Oct-2023	8.8	An issue discovered in Extreme Networks Switch Engine (EXOS) before 32.5.1.5, before 22.7 and before 31.7.1 allows attackers to gain escalated privileges via crafted HTTP request. **CVE ID : CVE-2023-43120**	https://extreme-networks.my.site.com/ExtrArticleDetail?an=000114377	O-EXT-EXOS-281123/3657
Affected Version(s): From (including) 31.7.0 Up to (excluding) 31.7.2					
Incorrect Authorization	16-Oct-2023	9.8	An Access Control issue discovered in Extreme Networks Switch Engine (EXOS) before 32.5.1.5, also fixed in 22.7, 31.7.2 allows attackers to gain escalated privileges using crafted telnet commands via Redis server. **CVE ID : CVE-2023-43119**	https://extreme-networks.my.site.com/ExtrArticleDetail?an=000114378	O-EXT-EXOS-281123/3658
Cross-Site Request Forgery (CSRF)	16-Oct-2023	8.8	Cross Site Request Forgery (CSRF) vulnerability in Chalet application in Extreme Networks Switch Engine (EXOS) before 32.5.1.5, fixed in 31.7.2 and 32.5.1.5 allows attackers to run	https://extreme-networks.my.site.com/ExtrArticleDetail?an=000114379	O-EXT-EXOS-281123/3659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code and cause other unspecified impacts via /jsonrpc API. **CVE ID : CVE-2023-43118**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Oct-2023	7.5	A Directory Traversal vulnerability discovered in Chalet application in Extreme Networks Switch Engine (EXOS) before 32.5.1.5, before 22.7, and before 31.7.2 allows attackers to read arbitrary files. **CVE ID : CVE-2023-43121**	https://extreme-networks.my.site.com/ExtrArticleDetail?an=000114376	O-EXT-EXOS-281123/3660
Affected Version(s): From (including) 32.0 Up to (excluding) 32.5.1.5					
Incorrect Authorization	16-Oct-2023	9.8	An Access Control issue discovered in Extreme Networks Switch Engine (EXOS) before 32.5.1.5, also fixed in 22.7, 31.7.2 allows attackers to gain escalated privileges using crafted telnet commands via Redis server. **CVE ID : CVE-2023-43119**	https://extreme-networks.my.site.com/ExtrArticleDetail?an=000114378	O-EXT-EXOS-281123/3661
Cross-Site Request	16-Oct-2023	8.8	Cross Site Request Forgery (CSRF) vulnerability in Chalet application	https://extreme-networks.my.site.com/ExtrArtic	O-EXT-EXOS-281123/3662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			in Extreme Networks Switch Engine (EXOS) before 32.5.1.5, fixed in 31.7.2 and 32.5.1.5 allows attackers to run arbitrary code and cause other unspecified impacts via /jsonrpc API. **CVE ID : CVE-2023-43118**	leDetail?an=000114379	
N/A	16-Oct-2023	8.8	An issue discovered in Extreme Networks Switch Engine (EXOS) before 32.5.1.5, before 22.7 and before 31.7.1 allows attackers to gain escalated privileges via crafted HTTP request. **CVE ID : CVE-2023-43120**	https://extreme-networks.my.site.com/ExtrArticleDetail?an=000114377	O-EXT-EXOS-281123/3663
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Oct-2023	7.5	A Directory Traversal vulnerability discovered in Chalet application in Extreme Networks Switch Engine (EXOS) before 32.5.1.5, before 22.7, and before 31.7.2 allows attackers to read arbitrary files.	https://extreme-networks.my.site.com/ExtrArticleDetail?an=000114376	O-EXT-EXOS-281123/3664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43121		
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 37					
Improper Input Validation	17-Oct-2023	7.5	Improper Input Validation vulnerability in Apache Traffic Server with malformed HTTP/2 frames.This issue affects Apache Traffic Server: from 9.0.0 through 9.2.2. Users are recommended to upgrade to version 9.2.3, which fixes the issue. **CVE ID : CVE-2023-39456**	https://lists.apache.org/thread/5py8h42mxfsn8l1wy6o41xwhsjlsd87q	O-FED-FEDO-281123/3665
Exposure of Sensitive Information to an Unauthorized Actor	17-Oct-2023	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Traffic Server.This issue affects Apache Traffic Server: from 8.0.0 through 8.1.8, from 9.0.0 through 9.2.2. Users are recommended to upgrade to version 8.1.9 or 9.2.3,	https://lists.apache.org/thread/5py8h42mxfsn8l1wy6o41xwhsjlsd87q	O-FED-FEDO-281123/3666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which fixes the issue. **CVE ID : CVE-2023-41752**		
Exposure of Resource to Wrong Sphere	18-Oct-2023	3.6	Redis is an in-memory database that persists on disk. On startup, Redis begins listening on a Unix socket before adjusting its permissions to the user-provided configuration. If a permissive umask(2) is used, this creates a race condition that enables, during a short period of time, another process to establish an otherwise unauthorized connection. This problem has existed since Redis 2.6.0-RC1. This issue has been addressed in Redis versions 7.2.2, 7.0.14 and 6.2.14. Users are advised to upgrade. For users unable to upgrade, it is possible to work around the problem by disabling Unix sockets, starting	https://github.com/redis/redis/commit/03345ddc7faf7af079485f2cbe5d17a1611cbce1, https://github.com/redis/redis/security/advisories/GHSA-ghmp-889m-7cvx	O-FED-FEDO-281123/3667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Redis with a restrictive umask, or storing the Unix socket file in a protected directory. **CVE ID : CVE-2023-45145**		
Missing Release of Memory after Effective Lifetime	30-Oct-2023	3.3	A memory leak flaw was found in ruby-magick, an interface between Ruby and ImageMagick. This issue can lead to a denial of service (DOS) by memory exhaustion. **CVE ID : CVE-2023-5349**	https://github.com/rmagick/rmagick/pull/1406	O-FED-FEDO-281123/3668
Affected Version(s): 38					
Use After Free	25-Oct-2023	8.8	Use after free in Profiles in Google Chrome prior to 118.0.5993.117 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-5472**	https://chromereleases.googleblog.com/2023/10/stable-channel-update-for-desktop_24.html	O-FED-FEDO-281123/3669
Out-of-bounds Write	25-Oct-2023	7.8	A out-of-bounds write flaw was found in the xorg-x11-server. This issue occurs due to an incorrect calculation of a	https://lists.x.org/archives/xorg-announce/2023-	O-FED-FEDO-281123/3670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer offset when copying data stored in the heap in the XIChangeDeviceProperty function in Xi/xiproperty.c and in RRChangeOutputProperty function in randr/rrproperty.c, allowing for possible escalation of privileges or denial of service. **CVE ID : CVE-2023-5367**	October/003430.html	
Out-of-bounds Read	23-Oct-2023	7.5	Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57. **CVE ID : CVE-2023-31122**	https://httpd.apache.org/security/vulnerabilities_24.html	O-FED-FEDO-281123/3671
Improper Input Validation	17-Oct-2023	7.5	Improper Input Validation vulnerability in Apache Traffic Server with malformed HTTP/2 frames.This issue affects Apache Traffic Server: from 9.0.0 through 9.2.2. Users are recommended to	https://lists.apache.org/thread/5py8h42mxfsn8l1wy6o41xwhsjlsd87q	O-FED-FEDO-281123/3672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade to version 9.2.3, which fixes the issue. **CVE ID : CVE-2023-39456**		
Exposure of Sensitive Information to an Unauthorized Actor	17-Oct-2023	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Traffic Server.This issue affects Apache Traffic Server: from 8.0.0 through 8.1.8, from 9.0.0 through 9.2.2. Users are recommended to upgrade to version 8.1.9 or 9.2.3, which fixes the issue. **CVE ID : CVE-2023-41752**	https://lists.apache.org/thread/5py8h42mxfsn8l1wy6o41xwhsjlsd87q	O-FED-FEDO-281123/3673
Uncontrolled Resource Consumption	23-Oct-2023	5.9	When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy	https://httpd.apache.org/security/vulnerabilities_24.html	O-FED-FEDO-281123/3674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue. **CVE ID : CVE-2023-45802**		
Use After Free	25-Oct-2023	4.7	A use-after-free flaw was found in the xorg-x11-server. An X server crash may occur in a very specific and	https://lists.x.org/archives/xorg-announce/2023-	O-FED-FEDO-281123/3675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			legacy configuration (a multi-screen setup with multiple protocol screens, also known as Zaphod mode) if the pointer is warped from within a window on one screen to the root window of the other screen and if the original window is destroyed followed by another window being destroyed. **CVE ID : CVE-2023-5380**	October/003430.html	
Exposure of Sensitive Information to an Unauthorized Actor	17-Oct-2023	4.2	urllib3 is a user-friendly HTTP client library for Python. urllib3 previously wouldn't remove the HTTP request body when an HTTP redirect response using status 301, 302, or 303 after the request had its method changed from one that could accept a request body (like `POST`) to `GET` as is required by HTTP RFCs. Although this behavior is not specified in the section for	https://github.com/urllib3/urllib3/commit/4e98d57809dacab1cbe625fddeec1a290c478ea9	O-FED-FEDO-281123/3676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			redirects, it can be inferred by piecing together information from different sections and we have observed the behavior in other major HTTP client implementations like curl and web browsers. Because the vulnerability requires a previously trusted service to become compromised in order to have an impact on confidentiality we believe the exploitability of this vulnerability is low. Additionally, many users aren't putting sensitive data in HTTP request bodies, if this is the case then this vulnerability isn't exploitable. Both of the following conditions must be true to be affected by this vulnerability: 1. Using urllib3 and submitting sensitive information in the HTTP request body (such as form data or JSON) and 2. The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			origin service is compromised and starts redirecting using 301, 302, or 303 to a malicious peer or the redirected-to service becomes compromised. This issue has been addressed in versions 1.26.18 and 2.0.7 and users are advised to update to resolve this issue. Users unable to update should disable redirects for services that aren't expecting to respond with redirects with `redirects=False` and disable automatic redirects with `redirects=False` and handle 301, 302, and 303 redirects manually by stripping the HTTP request body. **CVE ID : CVE-2023-45803**		
Exposure of Resource to Wrong Sphere	18-Oct-2023	3.6	Redis is an in-memory database that persists on disk. On startup, Redis begins listening on a Unix	https://github.com/redis/redis/commit/03345ddc7faf7af079485f2cbe5d17a1611cbce1,	O-FED-FEDO-281123/3677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			socket before adjusting its permissions to the user-provided configuration. If a permissive umask(2) is used, this creates a race condition that enables, during a short period of time, another process to establish an otherwise unauthorized connection. This problem has existed since Redis 2.6.0-RC1. This issue has been addressed in Redis versions 7.2.2, 7.0.14 and 6.2.14. Users are advised to upgrade. For users unable to upgrade, it is possible to work around the problem by disabling Unix sockets, starting Redis with a restrictive umask, or storing the Unix socket file in a protected directory. **CVE ID : CVE-2023-45145**	https://github.com/redis/redis/security/advisories/GHSA-ghmp-889m-7cvx	
Vendor: freshtomato					
Product: freshtomato					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2023.3					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Oct-2023	9.8	An OS command injection vulnerability exists in the httpd iperfrun.cgi functionality of FreshTomato 2023.3. A specially crafted HTTP request can lead to arbitrary command execution. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2023-3991**	N/A	O-FRE-FRES-281123/3678
Vendor: Google					
Product: android					
Affected Version(s): -					
Out-of-bounds Read	18-Oct-2023	7.5	In multiple functions of protocolembmsadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	https://source.android.com/security/bulletin/pixel/2023-10-01	O-GOO-ANDR-281123/3679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35656		
Out-of-bounds Read	18-Oct-2023	7.5	In Init of protocolnetadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-35663**	https://source.android.com/security/bulletin/pixel/2023-10-01	O-GOO-ANDR-281123/3680
Affected Version(s): 14.0					
Out-of-bounds Write	30-Oct-2023	8.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21356**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3681
Use After Free	30-Oct-2023	8.8	In Bluetooth, there is a possibility of	https://source.android.com/doc	O-GOO-ANDR-281123/3682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code-execution due to a use after free. This could lead to paired device escalation of privilege in the privileged Bluetooth process with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21361**	s/security/bulletin/android-14	
N/A	30-Oct-2023	7.8	In Activity Manager, there is a possible background activity launch 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. **CVE ID : CVE-2023-21351**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3683
Use After Free	30-Oct-2023	7.8	In libaudioclient, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with no additional	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21355**		
N/A	30-Oct-2023	7.8	In UWB Google, there is a possible way for a malicious app to masquerade as system app com.android.uwb.resources due to improperly used crypto. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21358**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3685
Missing Authorization	30-Oct-2023	7.8	In Telephony, there is a possible way for a guest user to change the preferred SIM due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. **CVE ID : CVE-2023-21373**		
N/A	30-Oct-2023	7.8	In System UI, there is a possible factory reset protection bypass 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. **CVE ID : CVE-2023-21374**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3687
Out-of-bounds Read	30-Oct-2023	7.5	In NFA, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21353**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3688
Out-of-bounds Write	30-Oct-2023	6.7	In Bluetooth, there is a possible out of bounds write due to improper input validation. This	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3689

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. **CVE ID : CVE-2023-21360**		
Observable Discrepancy	30-Oct-2023	5.5	In Media Projection, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21350**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3690
Out-of-bounds Read	30-Oct-2023	5.5	In NFA, 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	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. **CVE ID : CVE-2023-21352**		
Observable Discrepancy	30-Oct-2023	5.5	In Package Manager Service, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21354**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3692
N/A	30-Oct-2023	5.5	In ContactsProvider, there is a possible crash loop due to resource exhaustion. This could lead to local persistent denial of service in the Phone app with User execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21364**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	30-Oct-2023	5.5	In Scudo, there is a possible way for an attacker to predict heap allocation patterns due to insecure implementation/design. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21366**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3694
Out-of-bounds Read	30-Oct-2023	4.4	In NFC, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21357**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3695
Out-of-bounds Read	30-Oct-2023	4.4	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21359**		
Affected Version(s): 11.0					
N/A	27-Oct-2023	7.8	In onTaskAppeared of PipTaskOrganizer.java, there is a possible way to bypass background activity launch restrictions 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. **CVE ID : CVE-2023-40116**	https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3697
N/A	27-Oct-2023	7.8	In resetSettingsLocked of SettingsProvider.java, there is a possible lockscreen bypass due to a permissions bypass. This could lead to local escalation of privilege with no	https://android.googlesource.com/platform/frameworks/base/+/ff86ff28cf82124f8e65833a2dd8c319aea08945, https://android.googlesource.com/platform/packages/apps/S	O-GOO-ANDR-281123/3698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40117**	ettings/+/11815817de2f2d70fe842b108356a1bc75d44ffb	
N/A	27-Oct-2023	7.8	In multiple locations, there is a possible way to bypass user notification of foreground services 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. **CVE ID : CVE-2023-40120**	https://android.googlesource.com/platform/frameworks/base/+/d26544e5a4fd554b790b4d0c5964d9e95d9e626b, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3699
N/A	27-Oct-2023	7.8	In onCreate of ApnEditor.java, there is a possible way for a Guest user to change the APN due to a permission bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is	https://android.googlesource.com/platform/packages/apps/Settings/+/63d464c3fa5c7b9900448fef3844790756e557eb, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. **CVE ID : CVE-2023-40125**		
Out-of-bounds Write	27-Oct-2023	7.8	In several functions of xmlregexp.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40128**	https://android.googlesource.com/platform/external/libxml2/+/1ccf89b87a3969edd56956e2d447f896037c8be7, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3701
N/A	27-Oct-2023	7.8	In onBindingDied of CallRedirectionProcessor.java, there is a possible permission bypass due to a logic error in the code. This could lead to local escalation of privilege and background activity launch with no additional execution privileges needed. User interaction is not needed for exploitation.	https://android.googlesource.com/platform/packages/services/Telecomm/+/5b335401d1c8de7d1c85f4a0cf353f7f9fc30218, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-40130		
Use After Free	27-Oct-2023	7.8	In android_view_InputDevice_create of android_view_InputDevice.cpp, there is a possible way to execute arbitrary code due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40140**	https://android.googlesource.com/platform/frameworks/base/+/2d88a5c481df8986dbba2e02c5bf82f105b36243, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3703
Use After Free	27-Oct-2023	7	In GpuService of GpuService.cpp, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40131**	https://android.googlesource.com/platform/frameworks/native/+/0cda11569dd256ff3220b4fe44f861f8081d7116, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3704
Deserialization of Untrusted Data	27-Oct-2023	5.5	In appendEscapedSQLString of DatabaseUtils.java,	https://android.googlesource.com/platform/frameworks/base	O-GOO-ANDR-281123/3705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			there is a possible SQL injection due to unsafe deserialization. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40121**	/+/3287ac2d2565dc96bf6177967f8e3aed33954253, https://source.android.com/security/bulletin/2023-10-01	
N/A	27-Oct-2023	5.5	In updateActionViews of PipMenuView.java, there is a possible bypass of a multi user security boundary due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40123**	https://android.googlesource.com/platform/frameworks/base/+/7212a4bec2d2f1a74fa54a12a04255d6a183baa9, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3706
N/A	27-Oct-2023	5.5	In multiple locations of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.a	O-GOO-ANDR-281123/3707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40133**	ndroid.com/security/bulletin/2023-10-01	
Externally Controlled Reference to a Resource in Another Sphere	27-Oct-2023	5.5	In FillUi of FillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40139**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3708
N/A	27-Oct-2023	3.3	In multiple locations, there is a possible way to access screenshots due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is	https://android.googlesource.com/platform/packages/providers/MediaProvider/+/747431250612507e8289ae8eb1a56303e79ab678, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. **CVE ID : CVE-2023-40127**		
N/A	27-Oct-2023	3.3	In applyCustomDescription of SaveUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40135**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3710
N/A	27-Oct-2023	3.3	In setHeader of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40136**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Oct-2023	3.3	In multiple functions of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40137**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3712
N/A	27-Oct-2023	3.3	In FillUi of FillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40138**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3713
Affected Version(s): 12.0					
Out-of-bounds Write	27-Oct-2023	8.8	In build_read_multi_rsp of gatt_sr.cc, there is a possible	https://android.googlesource.com/platform/packages/modul	O-GOO-ANDR-281123/3714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			out of bounds write due to a heap buffer overflow. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40129**	es/Bluetooth/+/c0151aa3ba76c785b32c7f9d16c98febe53017b1, https://source.android.com/security/bulletin/2023-10-01	
N/A	27-Oct-2023	7.8	In onTaskAppeared of PipTaskOrganizer.java, there is a possible way to bypass background activity launch restrictions 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. **CVE ID : CVE-2023-40116**	https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3715
N/A	27-Oct-2023	7.8	In resetSettingsLocked of SettingsProvider.java, there is a possible lockscreen bypass due to a	https://android.googlesource.com/platform/frameworks/base/+/ff86ff28cf82124f8e65833a2dd8c319aea089	O-GOO-ANDR-281123/3716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40117**	45, https://android.googlesource.com/platform/packages/apps/Settings/+/11815817de2f2d70fe842b108356a1bc75d44ffb	
N/A	27-Oct-2023	7.8	In multiple locations, there is a possible way to bypass user notification of foreground services 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. **CVE ID : CVE-2023-40120**	https://android.googlesource.com/platform/frameworks/base/+/d26544e5a4fd554b790b4d0c5964d9e95d9e626b, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3717
N/A	27-Oct-2023	7.8	In onCreate of ApnEditor.java, there is a possible way for a Guest user to change the APN due to a permission bypass. This could lead to local escalation of privilege with no	https://android.googlesource.com/platform/packages/apps/Settings/+/63d464c3fa5c7b9900448fef3844790756e557eb, https://source.android.com/sec	O-GOO-ANDR-281123/3718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40125**	urity/bulletin/2023-10-01	
Out-of-bounds Write	27-Oct-2023	7.8	In several functions of xmlregexp.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40128**	https://android.googlesource.com/platform/external/libxml2/+/1ccf89b87a3969edd56956e2d447f896037c8be7, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3719
N/A	27-Oct-2023	7.8	In onBindingDied of CallRedirectionProcessor.java, there is a possible permission bypass due to a logic error in the code. This could lead to local escalation of privilege and background activity launch with no additional execution privileges needed. User interaction is	https://android.googlesource.com/platform/packages/services/Telecomm/+/5b335401d1c8de7d1c85f4a0cf353f7f9fc30218, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. **CVE ID : CVE-2023-40130**		
Use After Free	27-Oct-2023	7.8	In android_view_InputDevice_create of android_view_InputDevice.cpp, there is a possible way to execute arbitrary code due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40140**	https://android.googlesource.com/platform/frameworks/base/+/2d88a5c481df8986dbba2e02c5bf82f105b36243, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3721
Use After Free	27-Oct-2023	7	In GpuService of GpuService.cpp, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40131**	https://android.googlesource.com/platform/frameworks/native/+/0cda11569dd256ff3220b4fe44f861f8081d7116, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3722
Deserialization of	27-Oct-2023	5.5	In appendEscapedSQ	https://android.googlesource.c	O-GOO-ANDR-281123/3723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Data			LString of DatabaseUtils.java, there is a possible SQL injection due to unsafe deserialization. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40121**	om/platform/frameworks/base/+/3287ac2d2565dc96bf6177967f8e3aed33954253, https://source.android.com/security/bulletin/2023-10-01	
N/A	27-Oct-2023	5.5	In updateActionViews of PipMenuView.java, there is a possible bypass of a multi user security boundary due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40123**	https://android.googlesource.com/platform/frameworks/base/+/7212a4bec2d2f1a74fa54a12a04255d6a183baa9, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3724
N/A	27-Oct-2023	5.5	In multiple locations of DialogFillUi.java, there is a possible way to view another user's images due to a	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd50	O-GOO-ANDR-281123/3725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40133**	3f33, https://source.android.com/security/bulletin/2023-10-01	
Externally Controlled Reference to a Resource in Another Sphere	27-Oct-2023	5.5	In FillUi of FillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40139**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3726
N/A	27-Oct-2023	3.3	In multiple locations, there is a possible way to access screenshots due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is	https://android.googlesource.com/platform/packages/providers/MediaProvider/+/747431250612507e8289ae8eb1a56303e79ab678, https://source.android.com/sec	O-GOO-ANDR-281123/3727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. **CVE ID : CVE-2023-40127**	urity/bulletin/2023-10-01	
N/A	27-Oct-2023	3.3	In isFullScreen of FillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40134**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3728
N/A	27-Oct-2023	3.3	In applyCustomDescription of SaveUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40135**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Oct-2023	3.3	In setHeader of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40136**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3730
N/A	27-Oct-2023	3.3	In multiple functions of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40137**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3731
N/A	27-Oct-2023	3.3	In FillUi of FillUi.java, there is a possible way to view another user's images due to a confused	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115c	O-GOO-ANDR-281123/3732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40138**	c1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	
Affected Version(s): * Up to (excluding) 14.0					
Use After Free	30-Oct-2023	8.8	In Bluetooth, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege when connecting to a Bluetooth device with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21392**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3733
Observable Discrepancy	30-Oct-2023	7.8	In InputMethod, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local escalation of	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21337**		
Missing Authorization	30-Oct-2023	7.8	In Permission Manager, there is a possible way to bypass required permissions due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21341**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3735
N/A	30-Oct-2023	7.8	In sdksandbox, there is a possible strandhogg style overlay attack 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.	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21398		
N/A	30-Oct-2023	7.8	In Setup Wizard, there is a possible way to save a WiFi network due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21397**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3737
N/A	30-Oct-2023	7.8	In Activity Manager, there is a possible background activity launch due to a logic error in the code. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21396**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3738
Observable Discrepancy	30-Oct-2023	7.8	In Slice, there is a possible disclosure of installed applications due to side channel information	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21298**		
Missing Authorization	30-Oct-2023	7.8	In Settings, there is a possible way for the user to change SIM due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21393**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3740
Observable Discrepancy	30-Oct-2023	7.8	In Package Installer, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local escalation of privilege with no additional	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21324**		
Incorrect Authorization	30-Oct-2023	7.8	In Sim, there is a possible way to evade mobile preference restrictions due to a permission bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21390**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3742
Missing Authorization	30-Oct-2023	7.8	In Settings, there is a possible restriction bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21388**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	30-Oct-2023	7.8	In Package Installer, there is a possible way to determine whether an app is installed, without query permissions, due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21328**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3744
Use After Free	30-Oct-2023	7.8	In Media Resource Manager, there is a possible local arbitrary code execution due to use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21381**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3745
Missing Authorization	30-Oct-2023	7.8	In Telecomm, there is a possible way to silence the ring for calls of secondary users due to a missing permission	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21378**		
Missing Authorization	30-Oct-2023	7.8	In Settings, there is a possible bypass of profile owner restrictions due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21389**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3747
Integer Overflow or Wraparound	30-Oct-2023	7.8	In Sysproxy, there is a possible out of bounds write due to an integer underflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. **CVE ID : CVE-2023-21375**		
Out-of-bounds Read	30-Oct-2023	7.8	In libdexfile, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21372**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3749
Missing Authorization	30-Oct-2023	7.8	In Core, there is a possible way to forward calls without user knowledge due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21313**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3750
N/A	30-Oct-2023	7.8	In ActivityStarter, there is a possible background activity launch due	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to an unsafe PendingIntent. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21343**		
N/A	30-Oct-2023	7.8	In Speech, there is a possible way to bypass background activity launch 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. **CVE ID : CVE-2023-21342**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3752
Improper Input Validation	30-Oct-2023	7.5	In Messaging, there is a possible way to disable the messaging application due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed.	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. **CVE ID : CVE-2023-21391**		
N/A	30-Oct-2023	7.5	In Minikin, there is a possible way to trigger ANR by showing a malicious message due to resource exhaustion. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21339**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3754
Out-of-bounds Read	30-Oct-2023	7.5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21347**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3755
N/A	30-Oct-2023	7.3	In Print Service, there is a possible background	https://source.android.com/doc	O-GOO-ANDR-281123/3756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			activity launch 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 needed for exploitation. **CVE ID : CVE-2023-45780**	s/security/bulletin/android-14	
Out-of-bounds Write	30-Oct-2023	6.7	In Bluetooth, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21380**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3757
Integer Overflow or Wraparound	30-Oct-2023	6.7	In the Security Element API, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. **CVE ID : CVE-2023-21370**		
Integer Overflow or Wraparound	30-Oct-2023	6.7	In Secure Element, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21371**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3759
Out-of-bounds Write	30-Oct-2023	6.7	In Bluetooth, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21310**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3760
Out-of-bounds Read	30-Oct-2023	6.5	In Bluetooth, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote (proximal/adjacent	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3761

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. **CVE ID : CVE-2023-21315**		
Use After Free	30-Oct-2023	6.5	In Bluetooth, there is a possible out of bounds read due to a use after free. This could lead to remote information disclosure over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21395**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3762
Missing Authorization	30-Oct-2023	5.5	In Slice, there is a possible disclosure of installed packages due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21294		
N/A	30-Oct-2023	5.5	In SliceManagerService, there is a possible way to check if a content provider is installed due to a missing null check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21295**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3764
Observable Discrepancy	30-Oct-2023	5.5	In Permission, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. **CVE ID : CVE-2023-21296**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	30-Oct-2023	5.5	In Content, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21318**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3766
Observable Discrepancy	30-Oct-2023	5.5	In Package Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21299**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	30-Oct-2023	5.5	In PackageManager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21300**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3768
Observable Discrepancy	30-Oct-2023	5.5	In ActivityManagerService, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21301**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	30-Oct-2023	5.5	In Package Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21302**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3770
Observable Discrepancy	30-Oct-2023	5.5	In Content, here is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21303**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	30-Oct-2023	5.5	In Content, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21305**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3772
Observable Discrepancy	30-Oct-2023	5.5	In ContentService, there is a possible way to read installed sync content providers due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21306**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3773
Out-of-bounds Read	30-Oct-2023	5.5	In collapse of canonicalize_md.c, there is a possible out of bounds read	https://source.android.com/doc	O-GOO-ANDR-281123/3774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-40101**	s/security/bulletin/android-14	
Out-of-bounds Read	30-Oct-2023	5.5	In Composer, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21308**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3775
Out-of-bounds Read	30-Oct-2023	5.5	In libcore, 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	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. **CVE ID : CVE-2023-21309**		
Incorrect Authorization	30-Oct-2023	5.5	In Settings, there is a possible way to control private DNS settings from a secondary user due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21311**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3777
N/A	30-Oct-2023	5.5	In IntentResolver, there is a possible cross-user media read due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21312**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3778
N/A	30-Oct-2023	5.5	In SELinux Policy, there is a possible restriction bypass	https://source.android.com/doc	O-GOO-ANDR-281123/3779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21377**	s/security/bulletin/android-14	
Observable Discrepancy	30-Oct-2023	5.5	In Content Service, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21304**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3780
Observable Discrepancy	30-Oct-2023	5.5	In Content, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21316**		
Observable Discrepancy	30-Oct-2023	5.5	In ContentService, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21317**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3782
Missing Authorization	30-Oct-2023	5.5	In Telecomm, there is a possible way to get the call state due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. **CVE ID : CVE-2023-21340**		
Observable Discrepancy	30-Oct-2023	5.5	In Input Method, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21338**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3784
Observable Discrepancy	30-Oct-2023	5.5	In Input Method, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21336		
Observable Discrepancy	30-Oct-2023	5.5	In Settings, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21335**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3786
Observable Discrepancy	30-Oct-2023	5.5	In Job Scheduler, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21344**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	30-Oct-2023	5.5	In App Ops Service, there is a possible disclosure of information about installed packages due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21334**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3788
N/A	30-Oct-2023	5.5	In Usage, there is a possible permanent DoS 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. **CVE ID : CVE-2023-21362**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3789
N/A	30-Oct-2023	5.5	In ContactsProvider, there is a possible crash loop due to resource exhaustion. This could lead to local persistent denial of service in the Phone app with	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21364**		
N/A	30-Oct-2023	5.5	In Contacts, there is a possible crash loop due to resource exhaustion. This could lead to local denial of service in the Phone app with User execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21365**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3791
N/A	30-Oct-2023	5.5	In Scudo, there is a possible way for an attacker to predict heap allocation patterns due to insecure implementation/design. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21366**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	30-Oct-2023	5.5	In Scudo, there is a possible way to exploit certain heap OOB read/write issues due to an insecure implementation/design. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21367**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3793
Out-of-bounds Read	30-Oct-2023	5.5	In Audio, there is a possible out of bounds read due to missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21368**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3794
N/A	30-Oct-2023	5.5	In Usage Access, there is a possible way to display a Settings usage access restriction toggle screen due to a permissions bypass. This could	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local denial of service with no additional execution privileges needed. User interaction is needed for exploitation. **CVE ID : CVE-2023-21369**		
Observable Discrepancy	30-Oct-2023	5.5	In Text Services, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21333**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3796
Observable Discrepancy	30-Oct-2023	5.5	In Text Services, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21332**		
N/A	30-Oct-2023	5.5	In Telephony, there is a possible way to retrieve the ICCID due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21376**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3798
Observable Discrepancy	30-Oct-2023	5.5	In InputMethod, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21331		
Observable Discrepancy	30-Oct-2023	5.5	In Overlay Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21330**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3800
Missing Authorization	30-Oct-2023	5.5	In Activity Manager, there is a possible way to determine whether an app is installed due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21329**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	30-Oct-2023	5.5	In Content Resolver, there is a possible method to access metadata about existing content providers on the device due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21382**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3802
N/A	30-Oct-2023	5.5	In Settings, there is a possible way for the user to unintentionally send extra data due to an unclear prompt. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. **CVE ID : CVE-2023-21383**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3803
N/A	30-Oct-2023	5.5	In Package Manager, there is a possible possible permissions bypass due to an	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21384**		
Out-of-bounds Write	30-Oct-2023	5.5	In Whitechapel, there is a possible out of bounds read due to memory corruption. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21385**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3805
Observable Discrepancy	30-Oct-2023	5.5	In Permission Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21327**		
Observable Discrepancy	30-Oct-2023	5.5	In PackageManagerNative, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21293**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3807
Observable Discrepancy	30-Oct-2023	5.5	In Package Manager Service, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21326**		
Observable Discrepancy	30-Oct-2023	5.5	In Settings, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21325**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3809
Observable Discrepancy	30-Oct-2023	5.5	In Activity Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. **CVE ID : CVE-2023-21323**		
Missing Authorization	30-Oct-2023	5.5	In Package Manager, there is a possible cross-user settings disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21321**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3811
N/A	30-Oct-2023	5.5	In Telecomm, there is a possible bypass of a multi user security boundary due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21394**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3812
Observable Discrepancy	30-Oct-2023	5.5	In Device Policy, there is a possible way to verify if a particular admin	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			app is registered on the device due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21320**		
Observable Discrepancy	30-Oct-2023	5.5	In UsageStatsService, there is a possible way to read installed 3rd party apps due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21319**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3814
Improper Authentication	30-Oct-2023	5	In Bluetooth, there is a possible way for a paired Bluetooth device to access a long term identifier for an Android device due	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. **CVE ID : CVE-2023-21307**		
Improper Authentication	30-Oct-2023	4.4	In SEPolicy, there is a possible way to access the factory MAC address due to a permissions bypass. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21297**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3816
Out-of-bounds Read	30-Oct-2023	4.4	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21314		
Insertion of Sensitive Information into Log File	30-Oct-2023	4.4	In User Backup Manager, there is a possible way to leak a token to bypass user confirmation for backup due to log information disclosure. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21387**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3818
Out-of-bounds Read	30-Oct-2023	4.4	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21379**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3819
Observable Discrepancy	30-Oct-2023	3.3	In Game Manager Service, there is a possible way to determine whether	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21345**		
Observable Discrepancy	30-Oct-2023	3.3	In the Device Idle Controller, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21346**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3821
Observable Discrepancy	30-Oct-2023	3.3	In Window Manager, there is a possible way to determine whether an app is installed,	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21348**		
Observable Discrepancy	30-Oct-2023	3.3	In Package Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-21349**	https://source.android.com/docs/security/bulletin/android-14	O-GOO-ANDR-281123/3823
Affected Version(s): 12.1					
Out-of-bounds Write	27-Oct-2023	8.8	In build_read_multi_rsp of gatt_sr.cc, there is a possible	https://android.googlesource.com/platform/packages/modul	O-GOO-ANDR-281123/3824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			out of bounds write due to a heap buffer overflow. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40129**	es/Bluetooth/+/c0151aa3ba76c785b32c7f9d16c98febe53017b1, https://source.android.com/security/bulletin/2023-10-01	
N/A	27-Oct-2023	7.8	In onTaskAppeared of PipTaskOrganizer.java, there is a possible way to bypass background activity launch restrictions 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. **CVE ID : CVE-2023-40116**	https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3825
N/A	27-Oct-2023	7.8	In resetSettingsLocked of SettingsProvider.java, there is a possible lockscreen bypass due to a	https://android.googlesource.com/platform/frameworks/base/+/ff86ff28cf82124f8e65833a2dd8c319aea089	O-GOO-ANDR-281123/3826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40117**	45, https://android.googlesource.com/platform/packages/apps/Settings/+/11815817de2f2d70fe842b108356a1bc75d44ffb	
N/A	27-Oct-2023	7.8	In multiple locations, there is a possible way to bypass user notification of foreground services 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. **CVE ID : CVE-2023-40120**	https://android.googlesource.com/platform/frameworks/base/+/d26544e5a4fd554b790b4d0c5964d9e95d9e626b, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3827
N/A	27-Oct-2023	7.8	In onCreate of ApnEditor.java, there is a possible way for a Guest user to change the APN due to a permission bypass. This could lead to local escalation of privilege with no	https://android.googlesource.com/platform/packages/apps/Settings/+/63d464c3fa5c7b9900448fef3844790756e557eb, https://source.android.com/sec	O-GOO-ANDR-281123/3828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40125**	urity/bulletin/2023-10-01	
Out-of-bounds Write	27-Oct-2023	7.8	In several functions of xmlregexp.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40128**	https://android.googlesource.com/platform/external/libxml2/+/1ccf89b87a3969edd56956e2d447f896037c8be7, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3829
N/A	27-Oct-2023	7.8	In onBindingDied of CallRedirectionProcessor.java, there is a possible permission bypass due to a logic error in the code. This could lead to local escalation of privilege and background activity launch with no additional execution privileges needed. User interaction is	https://android.googlesource.com/platform/packages/services/Telecomm/+/5b335401d1c8de7d1c85f4a0cf353f7f9fc30218, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. **CVE ID : CVE-2023-40130**		
Use After Free	27-Oct-2023	7.8	In android_view_InputDevice_create of android_view_InputDevice.cpp, there is a possible way to execute arbitrary code due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40140**	https://android.googlesource.com/platform/frameworks/base/+/2d88a5c481df8986dbba2e02c5bf82f105b36243, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3831
Use After Free	27-Oct-2023	7	In GpuService of GpuService.cpp, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40131**	https://android.googlesource.com/platform/frameworks/native/+/0cda11569dd256ff3220b4fe44f861f8081d7116, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3832
Deserialization of	27-Oct-2023	5.5	In appendEscapedSQ	https://android.googlesource.c	O-GOO-ANDR-281123/3833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Data			LString of DatabaseUtils.java, there is a possible SQL injection due to unsafe deserialization. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40121**	om/platform/frameworks/base/+/3287ac2d2565dc96bf6177967f8e3aed33954253, https://source.android.com/security/bulletin/2023-10-01	
N/A	27-Oct-2023	5.5	In updateActionViews of PipMenuView.java, there is a possible bypass of a multi user security boundary due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40123**	https://android.googlesource.com/platform/frameworks/base/+/7212a4bec2d2f1a74fa54a12a04255d6a183baa9, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3834
N/A	27-Oct-2023	5.5	In multiple locations of DialogFillUi.java, there is a possible way to view another user's images due to a	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd50	O-GOO-ANDR-281123/3835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40133**	3f33, https://source.android.com/security/bulletin/2023-10-01	
Externally Controlled Reference to a Resource in Another Sphere	27-Oct-2023	5.5	In FillUi of FillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40139**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3836
N/A	27-Oct-2023	3.3	In multiple locations, there is a possible way to access screenshots due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is	https://android.googlesource.com/platform/packages/providers/MediaProvider/+/747431250612507e8289ae8eb1a56303e79ab678, https://source.android.com/sec	O-GOO-ANDR-281123/3837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. **CVE ID : CVE-2023-40127**	urity/bulletin/2023-10-01	
N/A	27-Oct-2023	3.3	In isFullScreen of FillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40134**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3838
N/A	27-Oct-2023	3.3	In applyCustomDescription of SaveUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40135**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Oct-2023	3.3	In setHeader of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40136**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3840
N/A	27-Oct-2023	3.3	In multiple functions of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40137**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3841
N/A	27-Oct-2023	3.3	In FillUi of FillUi.java, there is a possible way to view another user's images due to a confused	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115c	O-GOO-ANDR-281123/3842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40138**	c1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	
Affected Version(s): 13.0					
Out-of-bounds Write	27-Oct-2023	8.8	In build_read_multi_rsp of gatt_sr.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40129**	https://android.googlesource.com/platform/packages/modules/Bluetooth/+/c0151aa3ba76c785b32c7f9d16c98febe53017b1, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3843
N/A	27-Oct-2023	7.8	In resetSettingsLocked of SettingsProvider.java, there is a possible lockscreen bypass due to a permissions bypass. This could lead to local	https://android.googlesource.com/platform/frameworks/base/+/ff86ff28cf82124f8e65833a2dd8c319aea08945, https://android.googlesource.c	O-GOO-ANDR-281123/3844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40117**	om/platform/packages/apps/Settings/+/11815817de2f2d70fe842b108356a1bc75d44ffb	
N/A	27-Oct-2023	7.8	In multiple locations, there is a possible way to bypass user notification of foreground services 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. **CVE ID : CVE-2023-40120**	https://android.googlesource.com/platform/frameworks/base/+/d26544e5a4fd554b790b4d0c5964d9e95d9e626b, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3845
N/A	27-Oct-2023	7.8	In onCreate of ApnEditor.java, there is a possible way for a Guest user to change the APN due to a permission bypass. This could lead to local escalation of privilege with no additional execution privileges needed.	https://android.googlesource.com/platform/packages/apps/Settings/+/63d464c3fa5c7b9900448fef3844790756e557eb, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. **CVE ID : CVE-2023-40125**		
Out-of-bounds Write	27-Oct-2023	7.8	In several functions of xmlregexp.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40128**	https://android.googlesource.com/platform/external/libxml2/+/1ccf89b87a3969edd56956e2d447f896037c8be7, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3847
N/A	27-Oct-2023	7.8	In onBindingDied of CallRedirectionProcessor.java, there is a possible permission bypass due to a logic error in the code. This could lead to local escalation of privilege and background activity launch with no additional execution privileges needed. User interaction is not needed for exploitation.	https://android.googlesource.com/platform/packages/services/Telecomm/+/5b335401d1c8de7d1c85f4a0cf353f7f9fc30218, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-40130		
Use After Free	27-Oct-2023	7.8	In android_view_InputDevice_create of android_view_InputDevice.cpp, there is a possible way to execute arbitrary code due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40140**	https://android.googlesource.com/platform/frameworks/base/+/2d88a5c481df8986dbba2e02c5bf82f105b36243, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3849
Use After Free	27-Oct-2023	7	In GpuService of GpuService.cpp, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40131**	https://android.googlesource.com/platform/frameworks/native/+/0cda11569dd256ff3220b4fe44f861f8081d7116, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3850
Deserialization of Untrusted Data	27-Oct-2023	5.5	In appendEscapedSQLString of DatabaseUtils.java,	https://android.googlesource.com/platform/frameworks/base	O-GOO-ANDR-281123/3851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			there is a possible SQL injection due to unsafe deserialization. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40121**	/+/3287ac2d2565dc96bf6177967f8e3aed33954253, https://source.android.com/security/bulletin/2023-10-01	
N/A	27-Oct-2023	5.5	In updateActionViews of PipMenuView.java, there is a possible bypass of a multi user security boundary due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40123**	https://android.googlesource.com/platform/frameworks/base/+/7212a4bec2d2f1a74fa54a12a04255d6a183baa9, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3852
N/A	27-Oct-2023	5.5	In multiple locations of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.a	O-GOO-ANDR-281123/3853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40133**	ndroid.com/security/bulletin/2023-10-01	
Externally Controlled Reference to a Resource in Another Sphere	27-Oct-2023	5.5	In FillUi of FillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40139**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3854
N/A	27-Oct-2023	3.3	In multiple locations, there is a possible way to access screenshots due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is	https://android.googlesource.com/platform/packages/providers/MediaProvider/+/747431250612507e8289ae8eb1a56303e79ab678, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. **CVE ID : CVE-2023-40127**		
N/A	27-Oct-2023	3.3	In isFullScreen of FillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40134**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3856
N/A	27-Oct-2023	3.3	In applyCustomDescription of SaveUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40135**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Oct-2023	3.3	In setHeader of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40136**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3858
N/A	27-Oct-2023	3.3	In multiple functions of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40137**	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115cc1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	O-GOO-ANDR-281123/3859
N/A	27-Oct-2023	3.3	In FillUi of FillUi.java, there is a possible way to view another user's images due to a confused	https://android.googlesource.com/platform/frameworks/base/+/08becc8c600f14c5529115c	O-GOO-ANDR-281123/3860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2023-40138**	c1a1e0c97cd503f33, https://source.android.com/security/bulletin/2023-10-01	
Vendor: govee					
Product: led_strip_firmware					
Affected Version(s): 3.00.42					
N/A	30-Oct-2023	7.5	An issue discovered in Govee LED Strip v3.00.42 allows attackers to cause a denial of service via crafted Move and MoveWithOnoff commands. **CVE ID : CVE-2023-45956**	N/A	O-GOV-LED_-281123/3861
Vendor: HP					
Product: 200_g4_22_all-in-one_pc_\(rom_family_ssid_86f0\)_firmware					
Affected Version(s): * Up to (excluding) f.50					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-200_-281123/3862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: 200_g4_22_all-in-one_pc_\(rom_family_ssid_86f2\)_firmware					
Affected Version(s): * Up to (excluding) f.50					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-200_-281123/3863
Product: 200_g4_22_all-in-one_pc_\(rom_family_ssid_86f3\)_firmware					
Affected Version(s): * Up to (excluding) f.50					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-200_-281123/3864
Product: 200_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f0\)_firmware					
Affected Version(s): * Up to (excluding) f.50					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-200_-281123/3865
Product: 200_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f2\)_firmware					
Affected Version(s): * Up to (excluding) f.50					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-200_-281123/3866
Product: 200_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f3\)_firmware					
Affected Version(s): * Up to (excluding) f.50					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-200_-281123/3867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: 205_g4_22_all-in-one_pc_\(rom_family_ssid_86f0\)_firmware					
Affected Version(s): * Up to (excluding) f.50					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-205_-281123/3868
Product: 205_g4_22_all-in-one_pc_\(rom_family_ssid_86f2\)_firmware					
Affected Version(s): * Up to (excluding) f.50					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability.	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-205_-281123/3869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26300		
Product: 205_g4_22_all-in-one_pc_\(rom_family_ssid_86f3\)_firmware					
Affected Version(s): * Up to (excluding) f.50					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-205_-281123/3870
Product: 205_g8_24_all-in-one_pc_\(rom_family_ssid_8923\)_firmware					
Affected Version(s): * Up to (excluding) f.20					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-205_-281123/3871
Product: 205_g8_24_all-in-one_pc_\(rom_family_ssid_8924\)_firmware					
Affected Version(s): * Up to (excluding) f.20					
N/A	18-Oct-2023	7.8	A potential security vulnerability has	https://support.hp.com/us-	O-HP-205_-281123/3872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	en/document/ish_9461800-9461828-16	
Product: 205_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f0\)_firmware					
Affected Version(s): * Up to (excluding) f.50					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-205_-281123/3873
Product: 205_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f2\)_firmware					
Affected Version(s): * Up to (excluding) f.50					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-205_-281123/3874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: 205_pro_g4_22_all-in-one_pc_\(rom_family_ssid_86f3\)_firmware					
Affected Version(s): * Up to (excluding) f.50					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-205_-281123/3875
Product: 205_pro_g8_24_all-in-one_pc_\(rom_family_ssid_8923\)_firmware					
Affected Version(s): * Up to (excluding) f.20					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-205_-281123/3876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 205_pro_g8_24_all-in-one_pc_\(rom_family_ssid_8924\)_firmware					
Affected Version(s): * Up to (excluding) f.20					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-205_-281123/3877
Product: 240_g10_firmware					
Affected Version(s): * Up to (excluding) f.05					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-240_-281123/3878
Product: 240_g6_firmware					
Affected Version(s): * Up to (excluding) f.55					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC	https://support.hp.com/us-en/document/i	O-HP-240_-281123/3879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	sh_9461800-9461828-16	
Product: 240_g7_firmware					
Affected Version(s): * Up to (excluding) f.75					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-240_-281123/3880
Product: 240_g9_firmware					
Affected Version(s): * Up to (excluding) f.06					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-240_-281123/3881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: 245_firmware					
Affected Version(s): * Up to (excluding) f.11					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-245_-281123/3882
Product: 245_g10_firmware					
Affected Version(s): * Up to (excluding) f.06					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-245_-281123/3883
Product: 245_g7_firmware					
Affected Version(s): * Up to (excluding) f.70					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-245_-281123/3884
Product: 245_g8_firmware					
Affected Version(s): * Up to (excluding) f.26					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-245_-281123/3885
Product: 245_g9_firmware					
Affected Version(s): * Up to (excluding) f.11					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-245_-281123/3886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: 246_g6_firmware					
Affected Version(s): * Up to (excluding) f.55					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-246_-281123/3887
Product: 246_g7_firmware					
Affected Version(s): * Up to (excluding) f.75					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability.	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-246_-281123/3888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26300		
Product: 247_g8_firmware					
Affected Version(s): * Up to (excluding) f.70					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-247_-281123/3889
Product: 250_g10_firmware					
Affected Version(s): * Up to (excluding) f.06					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-250_-281123/3890
Product: 250_g6_firmware					
Affected Version(s): * Up to (excluding) f.73					
N/A	18-Oct-2023	7.8	A potential security vulnerability has	https://support.hp.com/us-	O-HP-250_-281123/3891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	en/document/i sh_9461800-9461828-16	
Product: 250_g7_firmware					
Affected Version(s): * Up to (excluding) f.46					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-250_-281123/3892
Product: 250_g9_firmware					
Affected Version(s): * Up to (excluding) f.63					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-250_-281123/3893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: 255_g10_firmware					
Affected Version(s): * Up to (excluding) f.09					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-255_-281123/3894
Product: 255_g6_firmware					
Affected Version(s): * Up to (excluding) f.56					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-255_-281123/3895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 255_g7_firmware					
Affected Version(s): * Up to (excluding) f.41					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-255_-281123/3896
Product: 255_g8_firmware					
Affected Version(s): * Up to (excluding) f.37					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-255_-281123/3897
Product: 255_g8_\(rom_family_ssid_87d1\)_firmware					
Affected Version(s): * Up to (excluding) f.37					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC	https://support.hp.com/us-en/document/i	O-HP-255_-281123/3898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	sh_9461800-9461828-16	
Product: 255_g8_\(rom_family_ssid_8905\)_firmware					
Affected Version(s): * Up to (excluding) f.37					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-255_-281123/3899
Product: 255_g8_\(rom_family_ssid_890e\)_firmware					
Affected Version(s): * Up to (excluding) f.37					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-255_-281123/3900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: 255_g9_firmware					
Affected Version(s): * Up to (excluding) f.12					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-255_-281123/3901
Product: 256_g6_firmware					
Affected Version(s): * Up to (excluding) f.73					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-256_-281123/3902
Product: 256_g7_firmware					
Affected Version(s): * Up to (excluding) f.46					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-256_-281123/3903
Product: 258_g6_firmware					
Affected Version(s): * Up to (excluding) f.73					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-258_-281123/3904
Product: 258_g7_firmware					
Affected Version(s): * Up to (excluding) f.46					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-258_-281123/3905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: 285_g6_microtower_\(rom_family_ssid_871e\)_firmware					
Affected Version(s): * Up to (excluding) f.26					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-285_-281123/3906
Product: 285_g8_microtower_\(rom_family_ssid_870e\)_firmware					
Affected Version(s): * Up to (excluding) f.30					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability.	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-285_-281123/3907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26300		
Product: 285_pro_g6_microtower_\(rom_family_ssid_871e\)_firmware					
Affected Version(s): * Up to (excluding) f.26					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-285_-281123/3908
Product: 285_pro_g8_microtower_\(rom_family_ssid_870e\)_firmware					
Affected Version(s): * Up to (excluding) f.30					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-285_-281123/3909
Product: 295_g8_microtower_\(rom_family_ssid_870e\)_firmware					
Affected Version(s): * Up to (excluding) f.30					
N/A	18-Oct-2023	7.8	A potential security vulnerability has	https://support.hp.com/us-	O-HP-295_-281123/3910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	en/document/ish_9461800-9461828-16	
Product: 340_g7_firmware					
Affected Version(s): * Up to (excluding) f.39					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-340_-281123/3911
Product: 348_g7_firmware					
Affected Version(s): * Up to (excluding) f.39					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-348_-281123/3912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: 470_g10_firmware					
Affected Version(s): * Up to (excluding) f.03					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-470_-281123/3913
Product: 470_g7_firmware					
Affected Version(s): * Up to (excluding) f.70					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-470_-281123/3914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 470_g9_firmware					
Affected Version(s): * Up to (excluding) f.06					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-470_-281123/3915
Product: desktop_pro_a_300_g3_firmware					
Affected Version(s): * Up to (excluding) f.13					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-DESK-281123/3916
Product: desktop_pro_a_g3_firmware					
Affected Version(s): * Up to (excluding) f.13					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC	https://support.hp.com/us-en/document/i	O-HP-DESK-281123/3917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	sh_9461800-9461828-16	
Product: desktop_pro_a_g3_microtower_firmware					
Affected Version(s): * Up to (excluding) f.13					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-DESK-281123/3918
Product: proone_240_g10_\(rom_family_ssid_8b4c\)_firmware					
Affected Version(s): * Up to (excluding) f.05					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-PROO-281123/3919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: proone_240_g10_\(rom_family_ssid_8b4d\)_firmware					
Affected Version(s): * Up to (excluding) f.10					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-PROO-281123/3920
Product: proone_240_g9_\(rom_family_ssid_89eb\)_firmware					
Affected Version(s): * Up to (excluding) f.20					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-PROO-281123/3921
Product: pro_sff_280_g9_desktop_\(rom_family_ssid_89b4\)_firmware					
Affected Version(s): * Up to (excluding) f.22					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-PRO_-281123/3922
Product: pro_sff_280_g9_desktop_\(rom_family_ssid_8bc3\)_firmware					
Affected Version(s): * Up to (excluding) f.12					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-PRO_-281123/3923
Product: pro_sff_290_g9_desktop_\(rom_family_ssid_89b4\)_firmware					
Affected Version(s): * Up to (excluding) f.22					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-PRO_-281123/3924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: pro_sff_290_g9_desktop_\(rom_family_ssid_8bc3\)_firmware					
Affected Version(s): * Up to (excluding) f.12					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-PRO_-281123/3925
Product: pro_sff_zhan_66_g9_desktop_\(rom_family_ssid_89b4\)_firmware					
Affected Version(s): * Up to (excluding) f.22					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability.	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-PRO_-281123/3926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26300		
Product: pro_sff_zhan_66_g9_desktop_\(rom_family_ssid_8bc3\)_firmware					
Affected Version(s): * Up to (excluding) f.12					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-PRO_-281123/3927
Product: pro_tower_200_g9_desktop_\(rom_family_ssid_89b3\)_firmware					
Affected Version(s): * Up to (excluding) f.22					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-PRO_-281123/3928
Product: pro_tower_200_g9_desktop_\(rom_family_ssid_89b4\)_firmware					
Affected Version(s): * Up to (excluding) f.22					
N/A	18-Oct-2023	7.8	A potential security vulnerability has	https://support.hp.com/us-	O-HP-PRO_-281123/3929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	en/document/i sh_9461800-9461828-16	
Product: pro_tower_200_g9_desktop_\(rom_family_ssid_8bc3\)_firmware					
Affected Version(s): * Up to (excluding) f.12					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-PRO_-281123/3930
Product: pro_tower_280_g9_desktop_\(rom_family_ssid_89b3\)_firmware					
Affected Version(s): * Up to (excluding) f.22					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-PRO_-281123/3931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: pro_tower_280_g9_desktop_\(rom_family_ssid_89b4\)_firmware					
Affected Version(s): * Up to (excluding) f.22					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-PRO_-281123/3932
Product: pro_tower_290_g9_desktop_\(rom_family_ssid_89b3\)_firmware					
Affected Version(s): * Up to (excluding) f.22					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-PRO_-281123/3933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: pro_tower_290_g9_desktop_\(rom_family_ssid_89b4\)_firmware					
Affected Version(s): * Up to (excluding) f.22					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-PRO_-281123/3934
Product: pro_tower_290_g9_desktop_\(rom_family_ssid_8bc3\)_firmware					
Affected Version(s): * Up to (excluding) f.12					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-PRO_-281123/3935
Product: pro_tower_zhan_99_g9_desktop_\(rom_family_ssid_89b3\)_firmware					
Affected Version(s): * Up to (excluding) f.22					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC	https://support.hp.com/us-en/document/i	O-HP-PRO_-281123/3936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	sh_9461800-9461828-16	
Product: pro_tower_zhan_99_g9_desktop_\(rom_family_ssid_89b4\)_firmware					
Affected Version(s): * Up to (excluding) f.22					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-PRO_-281123/3937
Product: pro_tower_zhan_99_g9_desktop_\(rom_family_ssid_8b3c\)_firmware					
Affected Version(s): * Up to (excluding) f.12					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-PRO_-281123/3938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: stream_11_pro_g4_firmware					
Affected Version(s): * Up to (excluding) f.30					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-STRE-281123/3939
Product: stream_11_pro_g5_firmware					
Affected Version(s): * Up to (excluding) f.18					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-STRE-281123/3940
Product: t638_thin_client_firmware					
Affected Version(s): * Up to (excluding) 00.01.13					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-T638-281123/3941
Product: vr_backpack_g2_\(rom_family_ssid_8590\)_firmware					
Affected Version(s): * Up to (excluding) f.29					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-VR_B-281123/3942
Product: zbook_15_g5_mobile_workstation_firmware					
Affected Version(s): * Up to (excluding) f.37					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-ZBOO-281123/3943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Product: zhan_66_pro_a_g10_\(rom_family_ssid_8b4e\)_firmware					
Affected Version(s): * Up to (excluding) f.05					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-ZHAN-281123/3944
Product: zhan_66_pro_a_g1_r_microtower_firmware					
Affected Version(s): * Up to (excluding) f.13					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability.	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-ZHAN-281123/3945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26300		
Product: zhan_66_pro_a_g4_all-in-one_pc_\(rom_family_ssid_8923\)_firmware					
Affected Version(s): * Up to (excluding) f.20					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-ZHAN-281123/3946
Product: zhan_66_pro_a_g4_all-in-one_pc_\(rom_family_ssid_8924\)_firmware					
Affected Version(s): * Up to (excluding) f.20					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-ZHAN-281123/3947
Product: zhan_99_g3_mobile_workstation_firmware					
Affected Version(s): * Up to (excluding) f.19					
N/A	18-Oct-2023	7.8	A potential security vulnerability has	https://support.hp.com/us-	O-HP-ZHAN-281123/3948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	en/document/ish_9461800-9461828-16	
Product: zhan_99_g4_mobile_workstation_firmware					
Affected Version(s): * Up to (excluding) f.09					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-ZHAN-281123/3949
Product: zhan_99_pro_a_g2_microtower_\(rom_family_ssid_871e\)_firmware					
Affected Version(s): * Up to (excluding) f.20					
N/A	18-Oct-2023	7.8	A potential security vulnerability has been identified in the system BIOS for certain HP PC products which might allow escalation of privilege. HP is	https://support.hp.com/us-en/document/ish_9461800-9461828-16	O-HP-ZHAN-281123/3950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			releasing firmware updates to mitigate the potential vulnerability. **CVE ID : CVE-2023-26300**		
Vendor: hpe					
Product: integrated_lights-out_5_firmware					
Affected Version(s): * Up to (excluding) 2.98					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	O-HPE-INTE-281123/3951
Product: integrated_lights-out_6_firmware					
Affected Version(s): * Up to (excluding) 1.53					
N/A	18-Oct-2023	7.5	HPE Integrated Lights-Out 5, and Integrated Lights-Out 6 using iLOrest may cause denial of service. **CVE ID : CVE-2023-30911**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04544en_us	O-HPE-INTE-281123/3952
Vendor: IBM					
Product: aix					
Affected Version(s): -					
Uncontrolled Resource Consumption	25-Oct-2023	4.9	IBM TXSeries for Multiplatforms, 8.1, 8.2, and 9.1, CICS TX Standard CICS TX Advanced 10.1 and 11.1 could allow a privileged user to cause a denial of service	https://www.ibm.com/support/pages/node/7056429, https://exchange.xforce.ibmcloud.com/vulnerabilities/266061, https://www.ib	O-IBM-AIX-281123/3953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to uncontrolled resource consumption. IBM X-Force ID: 266016. **CVE ID : CVE-2023-42031**	m.com/support/pages/node/7056433	
Product: i					
Affected Version(s): 7.2					
N/A	16-Oct-2023	7.8	Backup, Recovery, and Media Services (BRMS) for IBM i 7.2, 7.3, and 7.4 contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain component access to the host operating system. IBM X-Force ID: 263583. **CVE ID : CVE-2023-40377**	https://exchange.xforce.ibmcloud.com/vulnerabilities/263583, https://www.ibm.com/support/pages/node/7048121	O-IBM-I-281123/3954
Improper Privilege Management	29-Oct-2023	7.8	Management Central as part of IBM i 7.2, 7.3, 7.4, and 7.5 Navigator contains a local privilege escalation vulnerability. A malicious actor with command line access to the operating system can exploit this	https://exchange.xforce.ibmcloud.com/vulnerabilities/264116, https://www.ibm.com/support/pages/node/7060686	O-IBM-I-281123/3955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to elevate privileges to gain root access to the operating system. IBM X-Force ID: 264116. **CVE ID : CVE-2023-40685**		
Improper Privilege Management	29-Oct-2023	7.8	Management Central as part of IBM i 7.2, 7.3, 7.4, and 7.5 Navigator contains a local privilege escalation vulnerability. A malicious actor with command line access to the operating system can exploit this vulnerability to elevate privileges to gain component access to the operating system. IBM X-Force ID: 264114. **CVE ID : CVE-2023-40686**	https://www.ibm.com/support/pages/node/7060686, https://exchange.xforce.ibmcloud.com/vulnerabilities/264114	O-IBM-I-281123/3956
Affected Version(s): 7.3					
N/A	16-Oct-2023	7.8	Backup, Recovery, and Media Services (BRMS) for IBM i 7.2, 7.3, and 7.4 contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate	https://exchange.xforce.ibmcloud.com/vulnerabilities/263583, https://www.ibm.com/support/pages/node/7048121	O-IBM-I-281123/3957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges to gain component access to the host operating system. IBM X-Force ID: 263583. **CVE ID : CVE-2023-40377**		
Improper Privilege Management	29-Oct-2023	7.8	Management Central as part of IBM i 7.2, 7.3, 7.4, and 7.5 Navigator contains a local privilege escalation vulnerability. A malicious actor with command line access to the operating system can exploit this vulnerability to elevate privileges to gain root access to the operating system. IBM X-Force ID: 264116. **CVE ID : CVE-2023-40685**	https://exchange.xforce.ibmcloud.com/vulnerabilities/264116, https://www.ibm.com/support/pages/node/7060686	O-IBM-I-281123/3958
Improper Privilege Management	29-Oct-2023	7.8	Management Central as part of IBM i 7.2, 7.3, 7.4, and 7.5 Navigator contains a local privilege escalation vulnerability. A malicious actor with command line access to the operating system can exploit this vulnerability to elevate privileges to gain component	https://www.ibm.com/support/pages/node/7060686, https://exchange.xforce.ibmcloud.com/vulnerabilities/264114	O-IBM-I-281123/3959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to the operating system. IBM X-Force ID: 264114. **CVE ID : CVE-2023-40686**		
Affected Version(s): 7.4					
N/A	16-Oct-2023	7.8	Backup, Recovery, and Media Services (BRMS) for IBM i 7.2, 7.3, and 7.4 contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain component access to the host operating system. IBM X-Force ID: 263583. **CVE ID : CVE-2023-40377**	https://exchange.xforce.ibmcloud.com/vulnerabilities/263583, https://www.ibm.com/support/pages/node/7048121	O-IBM-I-281123/3960
Improper Privilege Management	29-Oct-2023	7.8	Management Central as part of IBM i 7.2, 7.3, 7.4, and 7.5 Navigator contains a local privilege escalation vulnerability. A malicious actor with command line access to the operating system can exploit this vulnerability to elevate privileges to gain root access	https://exchange.xforce.ibmcloud.com/vulnerabilities/264116, https://www.ibm.com/support/pages/node/7060686	O-IBM-I-281123/3961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the operating system. IBM X-Force ID: 264116. **CVE ID : CVE-2023-40685**		
Improper Privilege Management	29-Oct-2023	7.8	Management Central as part of IBM i 7.2, 7.3, 7.4, and 7.5 Navigator contains a local privilege escalation vulnerability. A malicious actor with command line access to the operating system can exploit this vulnerability to elevate privileges to gain component access to the operating system. IBM X-Force ID: 264114. **CVE ID : CVE-2023-40686**	https://www.ibm.com/support/pages/node/7060686, https://exchange.xforce.ibmcloud.com/vulnerabilities/264114	O-IBM-I-281123/3962
Affected Version(s): 7.5					
Improper Privilege Management	29-Oct-2023	7.8	Management Central as part of IBM i 7.2, 7.3, 7.4, and 7.5 Navigator contains a local privilege escalation vulnerability. A malicious actor with command line access to the operating system can exploit this vulnerability to elevate privileges to gain root access	https://exchange.xforce.ibmcloud.com/vulnerabilities/264116, https://www.ibm.com/support/pages/node/7060686	O-IBM-I-281123/3963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the operating system. IBM X-Force ID: 264116. **CVE ID : CVE-2023-40685**		
Improper Privilege Management	29-Oct-2023	7.8	Management Central as part of IBM i 7.2, 7.3, 7.4, and 7.5 Navigator contains a local privilege escalation vulnerability. A malicious actor with command line access to the operating system can exploit this vulnerability to elevate privileges to gain component access to the operating system. IBM X-Force ID: 264114. **CVE ID : CVE-2023-40686**	https://www.ibm.com/support/pages/node/7060686, https://exchange.xforce.ibmcloud.com/vulnerabilities/264114	O-IBM-I-281123/3964
Vendor: Lenovo					
Product: thinkagile_hx1021_edg_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3965
Product: thinkagile_hx1320_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3966
Product: thinkagile_hx1321_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3967
Product: thinkagile_hx1331_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3968
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3970
Product: thinkagile_hx1520-r_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3971
Product: thinkagile_hx1521-r_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3972
Product: thinkagile_hx2320-e_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3973
Product: thinkagile_hx2321_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3974
Product: thinkagile_hx2330_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4607		
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3976
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3977
Product: thinkagile_hx2331_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3978
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3979
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinkagile_hx2720-e_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3981
Product: thinkagile_hx3320_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3982
Product: thinkagile_hx3321_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3983
Product: thinkagile_hx3330_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3984
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3985
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC;	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinkagile_hx3331_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3987
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3988
Improper Neutralization of Special Elements used in an SQL Command	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinkagile_hx3375_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3990
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3991
Improper Neutralization of Special	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind	https://support.lenovo.com/us/en/product_se	O-LEN-THIN-281123/3992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	curity/LEN-140960	
Product: thinkagile_hx3376_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3993
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3995
Product: thinkagile_hx3520-g_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3996
Product: thinkagile_hx3521-g_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3997
Product: thinkagile_hx3720_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3998
Product: thinkagile_hx3721_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/3999
Product: thinkagile_hx5520-c_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4000
Product: thinkagile_hx5520_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted API command. **CVE ID : CVE-2023-4607**		
Product: thinkagile_hx5521-c_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4002
Product: thinkagile_hx5521_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4003
Product: thinkagile_hx5530_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4005
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4006
Product: thinkagile_hx5531_firmware					
Affected Version(s): -					
Improper Privilege	25-Oct-2023	8.8	An authenticated XCC user can change	https://support.lenovo.com/us/en/product_se	O-LEN-THIN-281123/4007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4008
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4608		
Product: thinkagile_hx7520_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4010
Product: thinkagile_hx7521_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4011
Product: thinkagile_hx7530_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4012
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can	https://support.lenovo.com/us/en/product_se	O-LEN-THIN-281123/4013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	curity/LEN-140960	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4014
Product: thinkagile_hx7531_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted API command. **CVE ID : CVE-2023-4607**		
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4016
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: thinkagile_hx7820_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4018
Product: thinkagile_hx7821_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4019
Product: thinkagile_hx_enclosure_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4020
Product: thinkagile_mx1021_on_se350_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for	https://support.lenovo.com/us/en/product_se	O-LEN-THIN-281123/4021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			any user through a crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Product: thinkagile_mx3330-f_all-flash_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4022
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4023
Improper Neutralization of Special Elements used in an SQL	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinkagile_mx3330-h_hybrid_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4025
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4606		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4027
Product: thinkagile_mx3331-f_all-flash_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4028
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4030
Product: thinkagile_mx3331-h_hybrid_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4032
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4033
Product: thinkagile_mx3530-h_hybrid_firmware					
Affected Version(s): -					
Improper Privilege	25-Oct-2023	8.8	An authenticated XCC user can change	https://support.lenovo.com/us/en/product_se	O-LEN-THIN-281123/4034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4035
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4608		
Product: thinkagile_mx3530_f_all_flash_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4037
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4038
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinkagile_mx3531-f_all-flash_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4040
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4041
Improper Neutralization of Special	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind	https://support.lenovo.com/us/en/product_se	O-LEN-THIN-281123/4042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	curity/LEN-140960	
Product: thinkagile_mx3531_h_hybrid_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4043
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4606		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4045
Product: thinkagile_mx_edge-_mx1020__firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4046
Product: thinkagile_vx1320_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4607		
Product: thinkagile_vx2320_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4048
Product: thinkagile_vx2330_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4049
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4606		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4051
Product: thinkagile_vx3320_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4052
Product: thinkagile_vx3330_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4607		
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4054
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4055
Product: thinkagile_vx3331_firmware					
Affected Version(s): -					
Improper Privilege	25-Oct-2023	8.8	An authenticated XCC user can change	https://support.lenovo.com/us/en/product_se	O-LEN-THIN-281123/4056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4057
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4058
Product: thinkagile_vx3520-g_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4059
Product: thinkagile_vx3530-g_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4060
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4061
Improper Neutralization of	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges	https://support.lenovo.com/us/en/product_se	O-LEN-THIN-281123/4062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	curity/LEN-140960	
Product: thinkagile_vx3720_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4063
Product: thinkagile_vx5520_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4064
Product: thinkagile_vx5530_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4065
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4066
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4608		
Product: thinkagile_vx7320_n_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4068
Product: thinkagile_vx7330_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4069
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4606		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4071
Product: thinkagile_vx7520_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4072
Product: thinkagile_vx7520_n_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4607		
Product: thinkagile_vx7530_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4074
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4075
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinkagile_vx7531_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4077
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4078
Improper Neutralization of Special Elements used in an SQL	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinkagile_vx7820_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4080
Product: thinkagile_vx_1se_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4081
Product: thinkagile_vx_2u4n_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a	https://support.lenovo.com/us/en/product_se	O-LEN-THIN-281123/4082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Product: thinkagile_vx_4u_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4083
Product: thinkedge_se450__firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4084
Product: thinksystem_sd530_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4085
Product: thinksystem_sd630_v2_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4086
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4087
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinksystem_sd650-n_v2_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4089
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4090
Improper Neutralization of Special Elements used in an SQL Command	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinksystem_sd650_dual_node_tray_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4092
Product: thinksystem_sd650_dwc_dual_node_tray_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4093
Product: thinksystem_sd650_v2_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4607		
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4095
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4096
Product: thinksystem_sd650_v3_firmware					
Affected Version(s): -					
Improper Privilege	25-Oct-2023	8.8	An authenticated XCC user can change	https://support.lenovo.com/us/en/product_se	O-LEN-THIN-281123/4097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4098
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: thinksystem_sd665_v3_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4100
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4101
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC;	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinksystem_se350_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4103
Product: thinksystem_sn550_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4104
Product: thinksystem_sn550_v2_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4106
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4107
Product: thinksystem_sn850_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted API command. **CVE ID : CVE-2023-4607**		
Product: thinksystem_sr150_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4109
Product: thinksystem_sr158_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4110
Product: thinksystem_sr250_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4112
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4113
Product: thinksystem_sr258_firmware					
Affected Version(s): -					
Improper Privilege	25-Oct-2023	8.8	An authenticated XCC user can change	https://support.lenovo.com/us/en/product_se	O-LEN-THIN-281123/4114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Product: thinksystem_sr258_v2_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4115
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4116
Improper Neutralization of Special Elements used in an	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinksystem_sr530_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4118
Product: thinksystem_sr550_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4119
Product: thinksystem_sr570_firmware					
Affected Version(s): -					
Improper Privilege	25-Oct-2023	8.8	An authenticated XCC user can change	https://support.lenovo.com/us/en/product_se	O-LEN-THIN-281123/4120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Product: thinksystem_sr590_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4121
Product: thinksystem_sr630_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4122
Product: thinksystem_sr630_v2_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4124
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4125
Product: thinksystem_sr630_v3_firmware					
Affected Version(s): -					
Improper Privilege	25-Oct-2023	8.8	An authenticated XCC user can change	https://support.lenovo.com/us/en/product_se	O-LEN-THIN-281123/4126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4127
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4608		
Product: thinksystem_sr635_v3_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4129
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4130
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinksystem_sr645_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4132
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4133
Improper Neutralization of	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges	https://support.lenovo.com/us/en/product_se	O-LEN-THIN-281123/4134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	curity/LEN-140960	
Product: thinksystem_sr645_v3_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4135
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4137
Product: thinksystem_sr650_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4138
Product: thinksystem_sr650_v2_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted API command. **CVE ID : CVE-2023-4607**		
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4140
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: thinksystem_sr650_v3_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4142
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4143
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinksystem_sr655_v3_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4145
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4146
Improper Neutralization of Special Elements used in an	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinksystem_sr665_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4148
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4606		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4150
Product: thinksystem_sr665_v3_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4151
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4153
Product: thinksystem_sr670_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4155
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4156
Product: thinksystem_sr670_v2_firmware					
Affected Version(s): -					
Improper Privilege	25-Oct-2023	8.8	An authenticated XCC user can change	https://support.lenovo.com/us/en/product_se	O-LEN-THIN-281123/4157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	curity/LEN-140960	
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4158
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4608		
Product: thinksystem_sr675_v3_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4160
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4161
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinksystem_sr850p_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4163
Product: thinksystem_sr850_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4164
Product: thinksystem_sr850_v2_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4607		
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4166
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4167
Product: thinksystem_sr850_v3_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4168
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4169
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			servers are not affected. **CVE ID : CVE-2023-4608**		
Product: thinksystem_sr860_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4171
Product: thinksystem_sr860_v2_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4172
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4174
Product: thinksystem_sr860_v3_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4175
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4177
Product: thinksystem_sr950_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4607		
Product: thinksystem_st250_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4179
Product: thinksystem_st250_v2_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4180
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4606		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4182
Product: thinksystem_st258_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4183
Product: thinksystem_st258_v2_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4607		
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4185
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4186
Product: thinksystem_st550_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4187
Product: thinksystem_st650_v2_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4188
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4189
Improper Neutralization of	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges	https://support.lenovo.com/us/en/product_se	O-LEN-THIN-281123/4190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	curity/LEN-140960	
Product: thinksystem_st650_v3_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4191
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4193
Product: thinksystem_st658_v2_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command. **CVE ID : CVE-2023-4607**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4194
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4196
Product: thinksystem_st658_v3_firmware					
Affected Version(s): -					
Improper Privilege Management	25-Oct-2023	8.8	An authenticated XCC user can change permissions for any user through a crafted API command.	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4607		
Missing Authorization	25-Oct-2023	8.1	An authenticated XCC user with Read-Only permission can change a different user's password through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4606**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4198
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Oct-2023	7.2	An authenticated XCC user with elevated privileges can perform blind SQL injection in limited cases through a crafted API command. This affects ThinkSystem v2 and v3 servers with XCC; ThinkSystem v1 servers are not affected. **CVE ID : CVE-2023-4608**	https://support.lenovo.com/us/en/product_security/LEN-140960	O-LEN-THIN-281123/4199
Vendor: Linux					
Product: linux_kernel					

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')	30-Oct-2023	9.8	tinyfiledialogs (aka tiny file dialogs) before 3.15.0 allows shell metacharacters (such as a backquote or a dollar sign) in titles, messages, and other input data. NOTE: this issue exists because of an incomplete fix for CVE-2020-36767, which only considered single and double quote characters. **CVE ID : CVE-2023-47104**	https://sourceforge.net/p/tinyfiledialogs/code/ci/ac9f9f6d8cdf45ca8d9b4cf1f201ee472301e114/	O-LIN-LINU-281123/4200
N/A	25-Oct-2023	7.8	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level privileges on the Linux instance. **CVE ID : CVE-2023-43506**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt	O-LIN-LINU-281123/4201
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows	https://exchange.xforce.ibmclou	O-LIN-LINU-281123/4202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain databases. IBM X-Force ID: 253440. **CVE ID : CVE-2023-30987**	d.com/vulnerabilities/253440, https://www.ibm.com/support/pages/node/7047560	
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to denial of service with a specially crafted query. IBM X-Force ID: 254037. **CVE ID : CVE-2023-30991**	https://www.ibm.com/support/pages/node/7047499, https://exchange.xforce.ibmcloud.com/vulnerabilities/254037	O-LIN-LINU-281123/4203
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 and 11.5 is vulnerable to denial of service with a specially crafted ALTER TABLE statement. IBM X-Force ID: 261616. **CVE ID : CVE-2023-38720**	https://www.ibm.com/support/pages/node/7047489, https://exchange.xforce.ibmcloud.com/vulnerabilities/261616	O-LIN-LINU-281123/4204
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2	https://exchange.xforce.ibmcloud.com/vulnerab	O-LIN-LINU-281123/4205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted XML query statement. IBM X-Force ID: 262258. **CVE ID : CVE-2023-38728**	ilities/262258, https://www.ibm.com/support/pages/node/7047478	
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX, and Windows (includes Db2 Connect Server) 11.5 is vulnerable to a denial of service with a specially crafted SQL statement. IBM X-Force ID: 262613. **CVE ID : CVE-2023-38740**	https://exchange.xforce.ibmcloud.com/vulnerabilities/262613, https://www.ibm.com/support/pages/node/7047554	O-LIN-LINU-281123/4206
N/A	17-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to denial of service with a specially crafted SQL statement using External Tables. IBM X-Force ID: 263499. **CVE ID : CVE-2023-40372**	https://exchange.xforce.ibmcloud.com/vulnerabilities/263499, https://www.ibm.com/support/pages/node/7047561	O-LIN-LINU-281123/4207
N/A	17-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to	https://www.ibm.com/support/pages/node/7047563, https://exchang	O-LIN-LINU-281123/4208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service with a specially crafted query containing common table expressions. IBM X-Force ID: 263574. **CVE ID : CVE-2023-40373**	e.xforce.ibmcloud.com/vulnerabilities/263574	
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to denial of service with a specially crafted query statement. IBM X-Force ID: 263575. **CVE ID : CVE-2023-40374**	https://www.ibm.com/support/pages/node/7047261, https://exchange.xforce.ibmcloud.com/vulnerabilities/263575	O-LIN-LINU-281123/4209
Uncontrolled Resource Consumption	25-Oct-2023	4.9	IBM TXSeries for Multiplatforms, 8.1, 8.2, and 9.1, CICS TX Standard CICS TX Advanced 10.1 and 11.1 could allow a privileged user to cause a denial of service due to uncontrolled resource consumption. IBM X-Force ID: 266016. **CVE ID : CVE-2023-42031**	https://www.ibm.com/support/pages/node/7056429, https://exchange.xforce.ibmcloud.com/vulnerabilities/266061, https://www.ibm.com/support/pages/node/7056433	O-LIN-LINU-281123/4210
N/A	17-Oct-2023	4.4	IBM Db2 11.5 could allow a local user with special	https://www.ibm.com/support/pages/node/7	O-LIN-LINU-281123/4211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges to cause a denial of service during database deactivation on DPF. IBM X-Force ID: 261607. **CVE ID : CVE-2023-38719**	047558, https://exchange.xforce.ibmcloud.com/vulnerabilities/261607	
Affected Version(s): * Up to (excluding) 6.4.12					
N/A	16-Oct-2023	9.1	extract_user_to_sg in lib/scatterlist.c in the Linux kernel before 6.4.12 fails to unpin pages in a certain situation, as demonstrated by a WARNING for try_grab_page. **CVE ID : CVE-2023-40791**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=f443fd5af5dbd531f880d3645d5dd36976cf087f	O-LIN-LINU-281123/4212
Affected Version(s): * Up to (excluding) 6.5.4					
Use After Free	16-Oct-2023	7.8	The Linux kernel before 6.5.4 has an es1 use-after-free in fs/ext4/extents_status.c, related to ext4_es_insert_extent. **CVE ID : CVE-2023-45898**	https://github.com/torvalds/linux/commit/768d612f79822d30a1e7d132a4d4b05337ce42ec, https://www.spinics.net/lists/stable-commits/msg317086.html, https://lkml.org/lkml/2023/8/13/477	O-LIN-LINU-281123/4213
Affected Version(s): * Up to (excluding) 6.5.9					
N/A	27-Oct-2023	7	An issue was discovered in the Linux kernel before 6.5.9, exploitable by local users with	https://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.5.9,	O-LIN-LINU-281123/4214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			userspace access to MMIO registers. Incorrect access checking in the #VC handler and instruction emulation of the SEV-ES emulation of MMIO accesses could lead to arbitrary write access to kernel memory (and thus privilege escalation). This depends on a race condition through which userspace can replace an instruction before the #VC handler reads it. **CVE ID : CVE-2023-46813**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=b9cb9c45583b911e0db71d09caa6b56469eb2bdf	
Affected Version(s): * Up to (excluding) 6.6					
Use After Free	23-Oct-2023	7.8	The reference count changes made as part of the CVE-2023-33951 and CVE-2023-33952 fixes exposed a use-after-free flaw in the way memory objects were handled when they were being used to store a surface. When running inside a VMware guest with 3D acceleration enabled, a local,	https://bugzilla.redhat.com/show_bug.cgi?id=2245663	O-LIN-LINU-281123/4215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unprivileged user could potentially use this flaw to escalate their privileges. **CVE ID : CVE-2023-5633**		
Affected Version(s): * Up to (including) 6.5.9					
NULL Pointer Dereference	29-Oct-2023	4.7	An issue was discovered in the Linux kernel through 6.5.9. During a race with SQ thread exit, an io_uring/fdinfo.c io_uring_show_fdinfo NULL pointer dereference can occur. **CVE ID : CVE-2023-46862**	https://github.com/torvalds/linux/commit/7644b1a1c9a7ae8ab99175989bfc8676055edb46, https://bugzilla.kernel.org/show_bug.cgi?id=218032#c4	O-LIN-LINU-281123/4216
Affected Version(s): 6.6					
Use After Free	23-Oct-2023	7.8	The reference count changes made as part of the CVE-2023-33951 and CVE-2023-33952 fixes exposed a use-after-free flaw in the way memory objects were handled when they were being used to store a surface. When running inside a VMware guest with 3D acceleration enabled, a local, unprivileged user could potentially	https://bugzilla.redhat.com/show_bug.cgi?id=2245663	O-LIN-LINU-281123/4217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use this flaw to escalate their privileges. **CVE ID : CVE-2023-5633**		
Out-of-bounds Write	25-Oct-2023	7.8	A heap out-of-bounds write vulnerability in the Linux kernel's Linux Kernel Performance Events (perf) component can be exploited to achieve local privilege escalation. If perf_read_group() is called while an event's sibling_list is smaller than its child's sibling_list, it can increment or write to memory locations outside of the allocated buffer. We recommend upgrading past commit 32671e3799ca2e4590773fd0e63aaa4229e50c06. **CVE ID : CVE-2023-5717**	https://kernel.dance/32671e3799ca2e4590773fd0e63aaa4229e50c06, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/kernel/events?id=32671e3799ca2e4590773fd0e63aaa4229e50c06	O-LIN-LINU-281123/4218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.4 Up to (excluding) 6.6					
Out-of-bounds Write	25-Oct-2023	7.8	A heap out-of-bounds write vulnerability in the Linux kernel's Linux Kernel Performance Events (perf) component can be exploited to achieve local privilege escalation. If perf_read_group() is called while an event's sibling_list is smaller than its child's sibling_list, it can increment or write to memory locations outside of the allocated buffer. We recommend upgrading past commit 32671e3799ca2e4590773fd0e63aaa4229e50c06. **CVE ID : CVE-2023-5717**	https://kernel.dance/32671e3799ca2e4590773fd0e63aaa4229e50c06, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/kernel/events?id=32671e3799ca2e4590773fd0e63aaa4229e50c06	O-LIN-LINU-281123/4219
Vendor: Mercurycom					
Product: a15_firmware					
Affected Version(s): 1.0_20230818_1.0.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	25-Oct-2023	9.8	Mercury A15 V1.0 20230818_1.0.3 was discovered to contain a command execution vulnerability via the component cloudDeviceToken SuccCB. **CVE ID : CVE-2023-46518**	N/A	O-MER-A15_-281123/4220
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Out-of-bounds Write	18-Oct-2023	9.8	A stack-based buffer overflow vulnerability exists in NI System Configuration that could result in information disclosure and/or arbitrary code execution. Successful exploitation requires that an attacker can provide a specially crafted response. This affects NI System Configuration 2023 Q3 and all previous versions. **CVE ID : CVE-2023-4601**	https://www.ni.com/en/support/documentation/supplemental/23/stack-based-buffer-overflow-in-ni-system-configuration.html	O-MIC-WIND-281123/4221
Improper Privilege	27-Oct-2023	7.8	A local privilege escalation vulnerability in	https://psirt.global.sonicwall.com/vuln-	O-MIC-WIND-281123/4222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			SonicWall Directory Services Connector Windows MSI client 4.1.21 and earlier versions allows a local low-privileged user to gain system privileges through running the recovery feature. **CVE ID : CVE-2023-44219**	detail/SNWLID-2023-0016	
N/A	19-Oct-2023	7.8	A privilege escalation vulnerability exists within the Qumu Multicast Extension v2 before 2.0.63 for Windows. When a standard user triggers a repair of the software, a pop-up window opens with SYSTEM privileges. Standard users may use this to gain arbitrary code execution as SYSTEM. **CVE ID : CVE-2023-45883**	N/A	O-MIC-WIND-281123/4223
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially	https://exchange.xforce.ibmcloud.com/vulnerabilities/253440, https://www.ibm.com/support	O-MIC-WIND-281123/4224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted query on certain databases. IBM X-Force ID: 253440. **CVE ID : CVE-2023-30987**	/pages/node/7047560	
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to denial of service with a specially crafted query. IBM X-Force ID: 254037. **CVE ID : CVE-2023-30991**	https://www.ibm.com/support/pages/node/7047499, https://exchange.xforce.ibmcloud.com/vulnerabilities/254037	O-MIC-WIND-281123/4225
Improper Verification of Cryptographic Signature	27-Oct-2023	7.5	VMware Tools contains a SAML token signature bypass vulnerability. A malicious actor that has been granted Guest Operation Privileges https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-6A952214-0E5E-4CCF-9D2A-90948FF643EC.html in a target virtual machine may be able to elevate their privileges if that target virtual	https://www.vmware.com/security/advisories/VMSA-2023-0024.html, http://www.openwall.com/lists/oss-security/2023/10/27/1	O-MIC-WIND-281123/4226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			machine has been assigned a more privileged Guest Alias https://vdc-download.vmware.com/vmwb-repository/dcr-public/d1902b0e-d479-46bf-8ac9-cee0e31e8ec0/07ce8dbd-db48-4261-9b8f-c6d3ad8ba472/vim.vm.guest.AliasManager.html . **CVE ID : CVE-2023-34058**		
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 and 11.5 is vulnerable to denial of service with a specially crafted ALTER TABLE statement. IBM X-Force ID: 261616. **CVE ID : CVE-2023-38720**	https://www.ibm.com/support/pages/node/7047489, https://exchange.xforce.ibmcloud.com/vulnerabilities/261616	O-MIC-WIND-281123/4227
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted XML query statement. IBM X-Force ID: 262258.	https://exchange.xforce.ibmcloud.com/vulnerabilities/262258, https://www.ibm.com/support/pages/node/7047478	O-MIC-WIND-281123/4228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38728		
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX, and Windows (includes Db2 Connect Server) 11.5 is vulnerable to a denial of service with a specially crafted SQL statement. IBM X-Force ID: 262613. **CVE ID : CVE-2023-38740**	https://exchange.xforce.ibmcloud.com/vulnerabilities/262613, https://www.ibm.com/support/pages/node/7047554	O-MIC-WIND-281123/4229
N/A	17-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to denial of service with a specially crafted SQL statement using External Tables. IBM X-Force ID: 263499. **CVE ID : CVE-2023-40372**	https://exchange.xforce.ibmcloud.com/vulnerabilities/263499, https://www.ibm.com/support/pages/node/7047561	O-MIC-WIND-281123/4230
N/A	17-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to denial of service with a specially crafted query containing common table expressions. IBM X-Force ID: 263574.	https://www.ibm.com/support/pages/node/7047563, https://exchange.xforce.ibmcloud.com/vulnerabilities/263574	O-MIC-WIND-281123/4231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-40373		
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to denial of service with a specially crafted query statement. IBM X-Force ID: 263575. **CVE ID : CVE-2023-40374**	https://www.ibm.com/support/pages/node/7047261, https://exchange.xforce.ibmcloud.com/vulnerabilities/263575	O-MIC-WIND-281123/4232
Time-of-check Time-of-use (TOCTOU) Race Condition	25-Oct-2023	7	A logged in user may elevate its permissions by abusing a Time-of-Check to Time-of-Use (TOCTOU) race condition. When a particular process flow is initiated, an attacker can exploit this condition to gain unauthorized elevated privileges on the affected system. **CVE ID : CVE-2023-38041**	https://forums.ivanti.com/s/article/CVE-2023-38041-New-client-side-release-to-address-a-privilege-escalation-on-Windows-user-machines?language=en_US	O-MIC-WIND-281123/4233
N/A	25-Oct-2023	6.5	The executable file warning was not presented when downloading .msix, .msixbundle, .appx, and .appxbundle files, which can run commands on a user's computer.	https://www.mozilla.org/security/advisories/mfsa2023-45/, https://www.mozilla.org/security/advisories/mfsa2023-47/, https://www.mozilla.org/secur	O-MIC-WIND-281123/4234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: This issue only affected Windows operating systems. Other operating systems are unaffected. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1. **CVE ID : CVE-2023-5727**	ity/advisories/mfsa2023-46/, https://bugzilla.mozilla.org/show_bug.cgi?id=1847180	
N/A	17-Oct-2023	4.4	IBM Db2 11.5 could allow a local user with special privileges to cause a denial of service during database deactivation on DPF. IBM X-Force ID: 261607. **CVE ID : CVE-2023-38719**	https://www.ibm.com/support/pages/node/7047558, https://exchange.xforce.ibmcloud.com/vulnerabilities/261607	O-MIC-WIND-281123/4235
Vendor: nanoleaf					
Product: lightstrip_firmware					
Affected Version(s): 3.5.10					
N/A	31-Oct-2023	7.5	An issue discovered in Nanoleaf Light strip v3.5.10 allows attackers to cause a denial of service via crafted write binding attribute commands. **CVE ID : CVE-2023-45955**	N/A	O-NAN-LIGH-281123/4236
Vendor: nxp					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: uboot_secondary_program_loader					
Affected Version(s): * Up to (excluding) 2023.07					
Improper Preservation of Permissions	17-Oct-2023	7.8	A software vulnerability has been identified in the U-Boot Secondary Program Loader (SPL) before 2023.07 on select NXP i.MX 8M family processors. Under certain conditions, a crafted Flattened Image Tree (FIT) format structure can be used to overwrite SPL memory, allowing unauthenticated software to execute on the target, leading to privilege escalation. This affects i.MX 8M, i.MX 8M Mini, i.MX 8M Nano, and i.MX 8M Plus. **CVE ID : CVE-2023-39902**	https://community.nxp.com/t5/i-MX-Security/U-Boot-Secondary-Program-Loader-Authentication-Vulnerability-CVE/ta-p/1736196	O-NXP-UBOO-281123/4237
Vendor: opengroup					
Product: unix					
Affected Version(s): -					
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially	https://exchange.xforce.ibmcloud.com/vulnerabilities/253440, https://www.ibm.com/support	O-OPE-UNIX-281123/4238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted query on certain databases. IBM X-Force ID: 253440. **CVE ID : CVE-2023-30987**	/pages/node/7047560	
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to denial of service with a specially crafted query. IBM X-Force ID: 254037. **CVE ID : CVE-2023-30991**	https://www.ibm.com/support/pages/node/7047499, https://exchange.xforce.ibmcloud.com/vulnerabilities/254037	O-OPE-UNIX-281123/4239
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 and 11.5 is vulnerable to denial of service with a specially crafted ALTER TABLE statement. IBM X-Force ID: 261616. **CVE ID : CVE-2023-38720**	https://www.ibm.com/support/pages/node/7047489, https://exchange.xforce.ibmcloud.com/vulnerabilities/261616	O-OPE-UNIX-281123/4240
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted XML query	https://exchange.xforce.ibmcloud.com/vulnerabilities/262258, https://www.ibm.com/support/pages/node/7047478	O-OPE-UNIX-281123/4241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			statement. IBM X-Force ID: 262258. **CVE ID : CVE-2023-38728**		
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX, and Windows (includes Db2 Connect Server) 11.5 is vulnerable to a denial of service with a specially crafted SQL statement. IBM X-Force ID: 262613. **CVE ID : CVE-2023-38740**	https://exchange.xforce.ibmcloud.com/vulnerabilities/262613, https://www.ibm.com/support/pages/node/7047554	O-OPE-UNIX-281123/4242
N/A	17-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to denial of service with a specially crafted SQL statement using External Tables. IBM X-Force ID: 263499. **CVE ID : CVE-2023-40372**	https://exchange.xforce.ibmcloud.com/vulnerabilities/263499, https://www.ibm.com/support/pages/node/7047561	O-OPE-UNIX-281123/4243
N/A	17-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to denial of service with a specially crafted query containing common table expressions. IBM	https://www.ibm.com/support/pages/node/7047563, https://exchange.xforce.ibmcloud.com/vulnerabilities/263574	O-OPE-UNIX-281123/4244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X-Force ID: 263574. **CVE ID : CVE-2023-40373**		
N/A	16-Oct-2023	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to denial of service with a specially crafted query statement. IBM X-Force ID: 263575. **CVE ID : CVE-2023-40374**	https://www.ibm.com/support/pages/node/7047261, https://exchange.xforce.ibmcloud.com/vulnerabilities/263575	O-OPE-UNIX-281123/4245
N/A	17-Oct-2023	4.4	IBM Db2 11.5 could allow a local user with special privileges to cause a denial of service during database deactivation on DPF. IBM X-Force ID: 261607. **CVE ID : CVE-2023-38719**	https://www.ibm.com/support/pages/node/7047558, https://exchange.xforce.ibmcloud.com/vulnerabilities/261607	O-OPE-UNIX-281123/4246
Vendor: Oracle					
Product: solaris					
Affected Version(s): 10					
N/A	17-Oct-2023	3.1	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystem). Supported versions that are affected are 10 and 11. Difficult to exploit vulnerability	https://www.oracle.com/security-alerts/cpuoct2023.html	O-ORA-SOLA-281123/4247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated attacker with network access via rquota to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22128**		
Affected Version(s): 11					
N/A	17-Oct-2023	5.5	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker	https://www.oracle.com/security-alerts/cpuoct2023.html	O-ORA-SOLA-281123/4248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. Note: This vunlerability only affects SPARC Systems. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22129**		
N/A	17-Oct-2023	3.1	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystem). Supported versions that are affected are 10 and 11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via	https://www.oracle.com/security-alerts/cpuoct2023.html	O-ORA-SOLA-281123/4249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rquota to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22128**		
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 7.0					
Out-of-bounds Write	25-Oct-2023	7.8	A out-of-bounds write flaw was found in the xorg-x11-server. This issue occurs due to an incorrect calculation of a buffer offset when copying data stored in the heap in the XIChangeDeviceProperty function in Xi/xiproperty.c and	https://lists.x.org/archives/xorg-announce/2023-October/003430.html	O-RED-ENTE-281123/4250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in RRChangeOutputProperty function in randr/rrproperty.c, allowing for possible escalation of privileges or denial of service. **CVE ID : CVE-2023-5367**		
Use After Free	25-Oct-2023	7	A use-after-free flaw was found in xorg-x11-server-Xvfb. This issue occurs in Xvfb with a very specific and legacy configuration (a multi-screen setup with multiple protocol screens, also known as Zaphod mode). If the pointer is warped from a screen 1 to a screen 0, a use-after-free issue may be triggered during shutdown or reset of the Xvfb server, allowing for possible escalation of privileges or denial of service. **CVE ID : CVE-2023-5574**	https://lists.x.org/archives/xorg-announce/2023-October/003430.html	O-RED-ENTE-281123/4251
Use After Free	25-Oct-2023	4.7	A use-after-free flaw was found in the xorg-x11-server. An X server crash may occur in a very specific and	https://lists.x.org/archives/xorg-announce/2023-	O-RED-ENTE-281123/4252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			legacy configuration (a multi-screen setup with multiple protocol screens, also known as Zaphod mode) if the pointer is warped from within a window on one screen to the root window of the other screen and if the original window is destroyed followed by another window being destroyed. **CVE ID : CVE-2023-5380**	October/003430.html	
Affected Version(s): 8.0					
Out-of-bounds Write	25-Oct-2023	7.8	An out-of-bounds write flaw was found in grub2's NTFS filesystem driver. This issue may allow an attacker to present a specially crafted NTFS filesystem image, leading to grub's heap metadata corruption. In some circumstances, the attack may also corrupt the UEFI firmware heap metadata. As a result, arbitrary code execution and secure boot	N/A	O-RED-ENTE-281123/4253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protection bypass may be achieved. **CVE ID : CVE-2023-4692**		
Out-of-bounds Write	25-Oct-2023	7.8	A out-of-bounds write flaw was found in the xorg-x11-server. This issue occurs due to an incorrect calculation of a buffer offset when copying data stored in the heap in the XIChangeDeviceProperty function in Xi/xiproperty.c and in RRChangeOutputProperty function in randr/rrproperty.c, allowing for possible escalation of privileges or denial of service. **CVE ID : CVE-2023-5367**	https://lists.x.org/archives/xorg-announce/2023-October/003430.html	O-RED-ENTE-281123/4254
Use After Free	23-Oct-2023	7.8	The reference count changes made as part of the CVE-2023-33951 and CVE-2023-33952 fixes exposed a use-after-free flaw in the way memory objects were handled when they were being used to store a surface. When running inside a VMware	https://bugzilla.redhat.com/show_bug.cgi?id=2245663	O-RED-ENTE-281123/4255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			guest with 3D acceleration enabled, a local, unprivileged user could potentially use this flaw to escalate their privileges. **CVE ID : CVE-2023-5633**		
Use After Free	25-Oct-2023	4.7	A use-after-free flaw was found in the xorg-x11-server. An X server crash may occur in a very specific and legacy configuration (a multi-screen setup with multiple protocol screens, also known as Zaphod mode) if the pointer is warped from within a window on one screen to the root window of the other screen and if the original window is destroyed followed by another window being destroyed. **CVE ID : CVE-2023-5380**	https://lists.x.org/archives/xorg-announce/2023-October/003430.html	O-RED-ENTE-281123/4256
Out-of-bounds Read	25-Oct-2023	4.6	An out-of-bounds read flaw was found on grub2's NTFS filesystem driver. This issue may allow a physically present	N/A	O-RED-ENTE-281123/4257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to present a specially crafted NTFS file system image to read arbitrary memory locations. A successful attack allows sensitive data cached in memory or EFI variable values to be leaked, presenting a high Confidentiality risk. **CVE ID : CVE-2023-4693**		
Affected Version(s): 9.0					
Out-of-bounds Write	25-Oct-2023	7.8	An out-of-bounds write flaw was found in grub2's NTFS filesystem driver. This issue may allow an attacker to present a specially crafted NTFS filesystem image, leading to grub's heap metadata corruption. In some circumstances, the attack may also corrupt the UEFI firmware heap metadata. As a result, arbitrary code execution and secure boot protection bypass may be achieved.	N/A	O-RED-ENTE-281123/4258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4692		
Out-of-bounds Write	25-Oct-2023	7.8	A out-of-bounds write flaw was found in the xorg-x11-server. This issue occurs due to an incorrect calculation of a buffer offset when copying data stored in the heap in the XIChangeDeviceProperty function in Xi/xiproperty.c and in RRChangeOutputProperty function in randr/rrproperty.c , allowing for possible escalation of privileges or denial of service. **CVE ID : CVE-2023-5367**	https://lists.x.org/archives/xorg-announce/2023-October/003430.html	O-RED-ENTE-281123/4259
Use After Free	23-Oct-2023	7.8	The reference count changes made as part of the CVE-2023-33951 and CVE-2023-33952 fixes exposed a use-after-free flaw in the way memory objects were handled when they were being used to store a surface. When running inside a VMware guest with 3D acceleration	https://bugzilla.redhat.com/show_bug.cgi?id=2245663	O-RED-ENTE-281123/4260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabled, a local, unprivileged user could potentially use this flaw to escalate their privileges. **CVE ID : CVE-2023-5633**		
Use After Free	25-Oct-2023	4.7	A use-after-free flaw was found in the xorg-x11-server. An X server crash may occur in a very specific and legacy configuration (a multi-screen setup with multiple protocol screens, also known as Zaphod mode) if the pointer is warped from within a window on one screen to the root window of the other screen and if the original window is destroyed followed by another window being destroyed. **CVE ID : CVE-2023-5380**	https://lists.x.org/archives/xorg-announce/2023-October/003430.html	O-RED-ENTE-281123/4261
Out-of-bounds Read	25-Oct-2023	4.6	An out-of-bounds read flaw was found on grub2's NTFS filesystem driver. This issue may allow a physically present attacker to present a specially crafted	N/A	O-RED-ENTE-281123/4262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NTFS file system image to read arbitrary memory locations. A successful attack allows sensitive data cached in memory or EFI variable values to be leaked, presenting a high Confidentiality risk. **CVE ID : CVE-2023-4693**		
Vendor: sick					
Product: fx0-gent00000_firmware					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	O-SIC-FX0--281123/4263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: fx0-gent00010_firmware					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	O-SIC-FX0--281123/4264
Product: fx0-gent00030_firmware					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	O-SIC-FX0--281123/4265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**		
Product: fx0-gepr00000_firmware					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	O-SIC-FX0--281123/4266
Product: fx0-gepr00010_firmware					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi	https://sick.com/.well-known/csaf/wh	O-SIC-FX0--281123/4267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	ite/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	
Product: fx0-get00000_firmware					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	O-SIC-FX0--281123/4268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass by capture-replay. **CVE ID : CVE-2023-5246**		
Product: fx0-get00010_firmware					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	O-SIC-FX0--281123/4269
Product: fx0-gmod00000_firmware					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487,	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-	O-SIC-FX0--281123/4270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	known/csaf/white/2023/sca-2023-0011.json	
Product: fx0-gmod00010_firmware					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	O-SIC-FX0--281123/4271
Product: fx0-gmod00030_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	O-SIC-FX0--281123/4272
Product: fx0-gpnt00000_firmware					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	O-SIC-FX0--281123/4273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**		
Product: fx0-gpnt00010_firmware					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	O-SIC-FX0--281123/4274
Product: fx0-gpnt00030_firmware					
Affected Version(s): -					
Improper Authentication	23-Oct-2023	8.8	Authentication Bypass by Capture-replay in SICK Flexi Soft Gateways with	https://sick.com/.well-known/csaf/white/2023/sca-	O-SIC-FX0--281123/4275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Partnumbers 1044073, 1127717, 1130282, 1044074, 1121597, 1099832, 1051432, 1127487, 1069070, 1112296, 1044072, 1121596, 1099830 allows an unauthenticated remote attacker to potentially impact the availability, integrity and confidentiality of the gateways via an authentication bypass by capture-replay. **CVE ID : CVE-2023-5246**	2023-0011.pdf, https://sick.com/psirt, https://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json	
Vendor: sielco					
Product: analog_fm_transmitter_exc1000gt_firmware					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	O-SIE-ANAL-281123/4276
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A	N/A	O-SIE-ANAL-281123/4277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**		
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	O-SIE-ANAL-281123/4278
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single	N/A	O-SIE-ANAL-281123/4279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**		
Product: analog_fm_transmitter_exc1000gx_firmware					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	O-SIE-ANAL-281123/4280
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	O-SIE-ANAL-281123/4281
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via	N/A	O-SIE-ANAL-281123/4282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**		
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	O-SIE-ANAL-281123/4283
Product: analog_fm_transmitter_exc100gt_firmware					
Affected Version(s): -					
Improper Restriction of Excessive	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by	N/A	O-SIE-ANAL-281123/4284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Attempts			brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**		
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	O-SIE-ANAL-281123/4285
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user	N/A	O-SIE-ANAL-281123/4286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			visits a malicious web site. **CVE ID : CVE-2023-45317**		
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	O-SIE-ANAL-281123/4287
Product: analog_fm_transmitter_exc120gt_firmware					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	O-SIE-ANAL-281123/4288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	O-SIE-ANAL-281123/4289
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	O-SIE-ANAL-281123/4290
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can	N/A	O-SIE-ANAL-281123/4291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**		
Product: analog_fm_transmitter_exc120gx_firmware					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	O-SIE-ANAL-281123/4292
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	O-SIE-ANAL-281123/4293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	O-SIE-ANAL-281123/4294
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	O-SIE-ANAL-281123/4295
Product: analog_fm_transmitter_exc1600gx_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	O-SIE-ANAL-281123/4296
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	O-SIE-ANAL-281123/4297
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with	N/A	O-SIE-ANAL-281123/4298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**		
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	O-SIE-ANAL-281123/4299
Product: analog_fm_transmitter_exc2000gx_firmware					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter.	N/A	O-SIE-ANAL-281123/4300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-42769		
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	O-SIE-ANAL-281123/4301
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	O-SIE-ANAL-281123/4302
N/A	26-Oct-2023	6.5	The application suffers from improper access	N/A	O-SIE-ANAL-281123/4303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**		
Product: analog_fm_transmitter_exc3000gx_firmware					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	O-SIE-ANAL-281123/4304
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST	N/A	O-SIE-ANAL-281123/4305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to set a parameter. **CVE ID : CVE-2023-41966**		
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	O-SIE-ANAL-281123/4306
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters.	N/A	O-SIE-ANAL-281123/4307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45228		
Product: analog_fm_transmitter_exc300gt_firmware					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	O-SIE-ANAL-281123/4308
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	O-SIE-ANAL-281123/4309
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the	N/A	O-SIE-ANAL-281123/4310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**		
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	O-SIE-ANAL-281123/4311
Product: analog_fm_transmitter_exc300gx_firmware					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid	N/A	O-SIE-ANAL-281123/4312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**		
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	O-SIE-ANAL-281123/4313
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	O-SIE-ANAL-281123/4314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	O-SIE-ANAL-281123/4315
Product: analog_fm_transmitter_exc30gt_firmware					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	O-SIE-ANAL-281123/4316
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges	N/A	O-SIE-ANAL-281123/4317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**		
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	O-SIE-ANAL-281123/4318
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified	N/A	O-SIE-ANAL-281123/4319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameters. **CVE ID : CVE-2023-45228**		
Product: analog_fm_transmitter_exc5000gt_firmware					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	O-SIE-ANAL-281123/4320
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	O-SIE-ANAL-281123/4321
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any	N/A	O-SIE-ANAL-281123/4322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**		
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	O-SIE-ANAL-281123/4323
Product: analog_fm_transmitter_exc5000gx_firmware					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a	N/A	O-SIE-ANAL-281123/4324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**		
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	O-SIE-ANAL-281123/4325
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site.	N/A	O-SIE-ANAL-281123/4326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45317		
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	O-SIE-ANAL-281123/4327
Product: polyeco1000_firmware					
Affected Version(s): 1.9.3					
Session Fixation	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to a session hijack vulnerability due to the cookie being vulnerable to a brute force attack, lack of SSL, and the session being visible in requests. **CVE ID : CVE-2023-0897**	N/A	O-SIE-POLY-281123/4328
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an attacker escalating their privileges by modifying passwords in POST requests.	N/A	O-SIE-POLY-281123/4329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46661		
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an authentication bypass vulnerability due to an attacker modifying passwords in a POST request and gain unauthorized access to the affected device with administrative privileges. **CVE ID : CVE-2023-46665**	N/A	O-SIE-POLY-281123/4330
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	Sielco PolyEco1000 uses a weak set of default administrative credentials that can be easily guessed in remote password attacks and gain full control of the system. **CVE ID : CVE-2023-5754**	N/A	O-SIE-POLY-281123/4331
N/A	26-Oct-2023	9.1	Sielco PolyEco1000 is vulnerable to an improper access control vulnerability when the application provides direct access to objects based on user-supplied input. As a	N/A	O-SIE-POLY-281123/4332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result of this vulnerability attackers can bypass authorization and access resources behind protected pages. **CVE ID : CVE-2023-46664**		
N/A	26-Oct-2023	8.1	Sielco PolyEco1000 is vulnerable to an attacker bypassing authorization and accessing resources behind protected pages. The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. **CVE ID : CVE-2023-46663**	N/A	O-SIE-POLY-281123/4333
N/A	26-Oct-2023	7.5	Sielco PolyEco1000 is vulnerable to an information disclosure vulnerability due to improper access control enforcement. An unauthenticated remote attacker can exploit this via a specially crafted request to gain	N/A	O-SIE-POLY-281123/4334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to sensitive information. **CVE ID : CVE-2023-46662**		
Affected Version(s): 1.9.4					
Session Fixation	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to a session hijack vulnerability due to the cookie being vulnerable to a brute force attack, lack of SSL, and the session being visible in requests. **CVE ID : CVE-2023-0897**	N/A	O-SIE-POLY-281123/4335
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an attacker escalating their privileges by modifying passwords in POST requests. **CVE ID : CVE-2023-46661**	N/A	O-SIE-POLY-281123/4336
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an authentication bypass vulnerability due to an attacker modifying passwords in a POST request and gain unauthorized access to the affected device with	N/A	O-SIE-POLY-281123/4337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrative privileges. **CVE ID : CVE-2023-46665**		
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	Sielco PolyEco1000 uses a weak set of default administrative credentials that can be easily guessed in remote password attacks and gain full control of the system. **CVE ID : CVE-2023-5754**	N/A	O-SIE-POLY-281123/4338
N/A	26-Oct-2023	9.1	Sielco PolyEco1000 is vulnerable to an improper access control vulnerability when the application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources behind protected pages. **CVE ID : CVE-2023-46664**	N/A	O-SIE-POLY-281123/4339
N/A	26-Oct-2023	8.1	Sielco PolyEco1000 is vulnerable to an attacker bypassing authorization and accessing	N/A	O-SIE-POLY-281123/4340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resources behind protected pages. The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. **CVE ID : CVE-2023-46663**		
N/A	26-Oct-2023	7.5	Sielco PolyEco1000 is vulnerable to an information disclosure vulnerability due to improper access control enforcement. An unauthenticated remote attacker can exploit this via a specially crafted request to gain access to sensitive information. **CVE ID : CVE-2023-46662**	N/A	O-SIE-POLY-281123/4341
Affected Version(s): 10.19					
Session Fixation	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to a session hijack vulnerability due to the cookie being vulnerable to a brute force attack, lack of SSL, and the session being visible in requests.	N/A	O-SIE-POLY-281123/4342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0897		
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an attacker escalating their privileges by modifying passwords in POST requests. **CVE ID : CVE-2023-46661**	N/A	O-SIE-POLY-281123/4343
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an authentication bypass vulnerability due to an attacker modifying passwords in a POST request and gain unauthorized access to the affected device with administrative privileges. **CVE ID : CVE-2023-46665**	N/A	O-SIE-POLY-281123/4344
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	Sielco PolyEco1000 uses a weak set of default administrative credentials that can be easily guessed in remote password attacks and gain full control of the system. **CVE ID : CVE-2023-5754**	N/A	O-SIE-POLY-281123/4345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	26-Oct-2023	9.1	Sielco PolyEco1000 is vulnerable to an improper access control vulnerability when the application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources behind protected pages. **CVE ID : CVE-2023-46664**	N/A	O-SIE-POLY-281123/4346
N/A	26-Oct-2023	8.1	Sielco PolyEco1000 is vulnerable to an attacker bypassing authorization and accessing resources behind protected pages. The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. **CVE ID : CVE-2023-46663**	N/A	O-SIE-POLY-281123/4347
N/A	26-Oct-2023	7.5	Sielco PolyEco1000 is vulnerable to an information disclosure vulnerability due	N/A	O-SIE-POLY-281123/4348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to improper access control enforcement. An unauthenticated remote attacker can exploit this via a specially crafted request to gain access to sensitive information. **CVE ID : CVE-2023-46662**		
Affected Version(s): 2.0.6					
Session Fixation	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to a session hijack vulnerability due to the cookie being vulnerable to a brute force attack, lack of SSL, and the session being visible in requests. **CVE ID : CVE-2023-0897**	N/A	O-SIE-POLY-281123/4349
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an attacker escalating their privileges by modifying passwords in POST requests. **CVE ID : CVE-2023-46661**	N/A	O-SIE-POLY-281123/4350
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an authentication bypass vulnerability due to an attacker modifying passwords in a	N/A	O-SIE-POLY-281123/4351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			POST request and gain unauthorized access to the affected device with administrative privileges. **CVE ID : CVE-2023-46665**		
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	Sielco PolyEco1000 uses a weak set of default administrative credentials that can be easily guessed in remote password attacks and gain full control of the system. **CVE ID : CVE-2023-5754**	N/A	O-SIE-POLY-281123/4352
N/A	26-Oct-2023	9.1	Sielco PolyEco1000 is vulnerable to an improper access control vulnerability when the application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources behind protected pages. **CVE ID : CVE-2023-46664**	N/A	O-SIE-POLY-281123/4353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	26-Oct-2023	8.1	Sielco PolyEco1000 is vulnerable to an attacker bypassing authorization and accessing resources behind protected pages. The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. **CVE ID : CVE-2023-46663**	N/A	O-SIE-POLY-281123/4354
N/A	26-Oct-2023	7.5	Sielco PolyEco1000 is vulnerable to an information disclosure vulnerability due to improper access control enforcement. An unauthenticated remote attacker can exploit this via a specially crafted request to gain access to sensitive information. **CVE ID : CVE-2023-46662**	N/A	O-SIE-POLY-281123/4355
Product: polyeco300_firmware					
Affected Version(s): 10.19					
Session Fixation	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to a session hijack vulnerability due to the cookie being	N/A	O-SIE-POLY-281123/4356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to a brute force attack, lack of SSL, and the session being visible in requests. **CVE ID : CVE-2023-0897**		
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an attacker escalating their privileges by modifying passwords in POST requests. **CVE ID : CVE-2023-46661**	N/A	O-SIE-POLY-281123/4357
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an authentication bypass vulnerability due to an attacker modifying passwords in a POST request and gain unauthorized access to the affected device with administrative privileges. **CVE ID : CVE-2023-46665**	N/A	O-SIE-POLY-281123/4358
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	Sielco PolyEco1000 uses a weak set of default administrative credentials that can be easily guessed in remote password attacks and gain full	N/A	O-SIE-POLY-281123/4359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control of the system. **CVE ID : CVE-2023-5754**		
N/A	26-Oct-2023	9.1	Sielco PolyEco1000 is vulnerable to an improper access control vulnerability when the application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources behind protected pages. **CVE ID : CVE-2023-46664**	N/A	O-SIE-POLY-281123/4360
N/A	26-Oct-2023	8.1	Sielco PolyEco1000 is vulnerable to an attacker bypassing authorization and accessing resources behind protected pages. The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. **CVE ID : CVE-2023-46663**	N/A	O-SIE-POLY-281123/4361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	26-Oct-2023	7.5	Sielco PolyEco1000 is vulnerable to an information disclosure vulnerability due to improper access control enforcement. An unauthenticated remote attacker can exploit this via a specially crafted request to gain access to sensitive information. **CVE ID : CVE-2023-46662**	N/A	O-SIE-POLY-281123/4362
Affected Version(s): 2.0.0					
Session Fixation	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to a session hijack vulnerability due to the cookie being vulnerable to a brute force attack, lack of SSL, and the session being visible in requests. **CVE ID : CVE-2023-0897**	N/A	O-SIE-POLY-281123/4363
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an attacker escalating their privileges by modifying passwords in POST requests. **CVE ID : CVE-2023-46661**	N/A	O-SIE-POLY-281123/4364
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an authentication	N/A	O-SIE-POLY-281123/4365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass vulnerability due to an attacker modifying passwords in a POST request and gain unauthorized access to the affected device with administrative privileges. **CVE ID : CVE-2023-46665**		
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	Sielco PolyEco1000 uses a weak set of default administrative credentials that can be easily guessed in remote password attacks and gain full control of the system. **CVE ID : CVE-2023-5754**	N/A	O-SIE-POLY-281123/4366
N/A	26-Oct-2023	9.1	Sielco PolyEco1000 is vulnerable to an improper access control vulnerability when the application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources	N/A	O-SIE-POLY-281123/4367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behind protected pages. **CVE ID : CVE-2023-46664**		
N/A	26-Oct-2023	8.1	Sielco PolyEco1000 is vulnerable to an attacker bypassing authorization and accessing resources behind protected pages. The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. **CVE ID : CVE-2023-46663**	N/A	O-SIE-POLY-281123/4368
N/A	26-Oct-2023	7.5	Sielco PolyEco1000 is vulnerable to an information disclosure vulnerability due to improper access control enforcement. An unauthenticated remote attacker can exploit this via a specially crafted request to gain access to sensitive information. **CVE ID : CVE-2023-46662**	N/A	O-SIE-POLY-281123/4369
Affected Version(s): 2.0.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Session Fixation	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to a session hijack vulnerability due to the cookie being vulnerable to a brute force attack, lack of SSL, and the session being visible in requests. **CVE ID : CVE-2023-0897**	N/A	O-SIE-POLY-281123/4370
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an attacker escalating their privileges by modifying passwords in POST requests. **CVE ID : CVE-2023-46661**	N/A	O-SIE-POLY-281123/4371
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an authentication bypass vulnerability due to an attacker modifying passwords in a POST request and gain unauthorized access to the affected device with administrative privileges. **CVE ID : CVE-2023-46665**	N/A	O-SIE-POLY-281123/4372
Improper Restriction of Excessive	26-Oct-2023	9.8	Sielco PolyEco1000 uses a weak set of default administrative	N/A	O-SIE-POLY-281123/4373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Attempts			credentials that can be easily guessed in remote password attacks and gain full control of the system. **CVE ID : CVE-2023-5754**		
N/A	26-Oct-2023	9.1	Sielco PolyEco1000 is vulnerable to an improper access control vulnerability when the application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources behind protected pages. **CVE ID : CVE-2023-46664**	N/A	O-SIE-POLY-281123/4374
N/A	26-Oct-2023	8.1	Sielco PolyEco1000 is vulnerable to an attacker bypassing authorization and accessing resources behind protected pages. The application interface allows users to perform certain actions via HTTP requests without performing any	N/A	O-SIE-POLY-281123/4375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validity checks to verify the requests. **CVE ID : CVE-2023-46663**		
N/A	26-Oct-2023	7.5	Sielco PolyEco1000 is vulnerable to an information disclosure vulnerability due to improper access control enforcement. An unauthenticated remote attacker can exploit this via a specially crafted request to gain access to sensitive information. **CVE ID : CVE-2023-46662**	N/A	O-SIE-POLY-281123/4376
Product: polyeco500_firmware					
Affected Version(s): 1.7.0					
Session Fixation	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to a session hijack vulnerability due to the cookie being vulnerable to a brute force attack, lack of SSL, and the session being visible in requests. **CVE ID : CVE-2023-0897**	N/A	O-SIE-POLY-281123/4377
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an attacker escalating their privileges by modifying	N/A	O-SIE-POLY-281123/4378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passwords in POST requests. **CVE ID : CVE-2023-46661**		
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an authentication bypass vulnerability due to an attacker modifying passwords in a POST request and gain unauthorized access to the affected device with administrative privileges. **CVE ID : CVE-2023-46665**	N/A	O-SIE-POLY-281123/4379
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	Sielco PolyEco1000 uses a weak set of default administrative credentials that can be easily guessed in remote password attacks and gain full control of the system. **CVE ID : CVE-2023-5754**	N/A	O-SIE-POLY-281123/4380
N/A	26-Oct-2023	9.1	Sielco PolyEco1000 is vulnerable to an improper access control vulnerability when the application provides direct access to objects	N/A	O-SIE-POLY-281123/4381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources behind protected pages. **CVE ID : CVE-2023-46664**		
N/A	26-Oct-2023	8.1	Sielco PolyEco1000 is vulnerable to an attacker bypassing authorization and accessing resources behind protected pages. The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. **CVE ID : CVE-2023-46663**	N/A	O-SIE-POLY-281123/4382
N/A	26-Oct-2023	7.5	Sielco PolyEco1000 is vulnerable to an information disclosure vulnerability due to improper access control enforcement. An unauthenticated remote attacker can exploit this via a specially crafted request to gain	N/A	O-SIE-POLY-281123/4383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to sensitive information. **CVE ID : CVE-2023-46662**		
Affected Version(s): 10.16					
Session Fixation	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to a session hijack vulnerability due to the cookie being vulnerable to a brute force attack, lack of SSL, and the session being visible in requests. **CVE ID : CVE-2023-0897**	N/A	O-SIE-POLY-281123/4384
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an attacker escalating their privileges by modifying passwords in POST requests. **CVE ID : CVE-2023-46661**	N/A	O-SIE-POLY-281123/4385
N/A	26-Oct-2023	9.8	Sielco PolyEco1000 is vulnerable to an authentication bypass vulnerability due to an attacker modifying passwords in a POST request and gain unauthorized access to the affected device with administrative privileges.	N/A	O-SIE-POLY-281123/4386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46665		
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	Sielco PolyEco1000 uses a weak set of default administrative credentials that can be easily guessed in remote password attacks and gain full control of the system. **CVE ID : CVE-2023-5754**	N/A	O-SIE-POLY-281123/4387
N/A	26-Oct-2023	9.1	Sielco PolyEco1000 is vulnerable to an improper access control vulnerability when the application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources behind protected pages. **CVE ID : CVE-2023-46664**	N/A	O-SIE-POLY-281123/4388
N/A	26-Oct-2023	8.1	Sielco PolyEco1000 is vulnerable to an attacker bypassing authorization and accessing resources behind protected pages.	N/A	O-SIE-POLY-281123/4389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. **CVE ID : CVE-2023-46663**		
N/A	26-Oct-2023	7.5	Sielco PolyEco1000 is vulnerable to an information disclosure vulnerability due to improper access control enforcement. An unauthenticated remote attacker can exploit this via a specially crafted request to gain access to sensitive information. **CVE ID : CVE-2023-46662**	N/A	O-SIE-POLY-281123/4390
Product: radio_link_exc19_firmware					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and	N/A	O-SIE-RADI-281123/4391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulate the transmitter. **CVE ID : CVE-2023-42769**		
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**	N/A	O-SIE-RADI-281123/4392
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	O-SIE-RADI-281123/4393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST request with modified parameters. **CVE ID : CVE-2023-45228**	N/A	O-SIE-RADI-281123/4394
Product: radio_link_rtx19_firmware					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	26-Oct-2023	9.8	The cookie session ID is of insufficient length and can be exploited by brute force, which may allow a remote attacker to obtain a valid session, bypass authentication, and manipulate the transmitter. **CVE ID : CVE-2023-42769**	N/A	O-SIE-RADI-281123/4395
Improper Privilege Management	26-Oct-2023	8.8	The application suffers from a privilege escalation vulnerability. A user with read permissions can elevate privileges	N/A	O-SIE-RADI-281123/4396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by sending a HTTP POST to set a parameter. **CVE ID : CVE-2023-41966**		
Cross-Site Request Forgery (CSRF)	26-Oct-2023	8.8	The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site. **CVE ID : CVE-2023-45317**	N/A	O-SIE-RADI-281123/4397
N/A	26-Oct-2023	6.5	The application suffers from improper access control when editing users. A user with read permissions can manipulate users, passwords, and permissions by sending a single HTTP POST	N/A	O-SIE-RADI-281123/4398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request with modified parameters. **CVE ID : CVE-2023-45228**		
Vendor: Sonicwall					
Product: sonicos					
Affected Version(s): * Up to (excluding) 6.5.4.13-105n					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4399
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4400
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4402
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4403
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4404
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4406
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4407
Affected Version(s): * Up to (excluding) 6.5.4.4-44v-21-2340					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4408
Use of Hard-	17-Oct-2023	7.5	SonicOS Use of Hard-coded	https://psirt.global.sonicwall.co	O-SON-SONI-281123/4409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	m/vuln-detail/SNWLID-2023-0012	
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4410
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4411
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4413
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4414
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4415
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-41712		
Affected Version(s): * Up to (excluding) 7.0.1-5145					
Improper Privilege Management	17-Oct-2023	8.8	SonicOS post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel allows users to elevate their privileges inside the tunnel. **CVE ID : CVE-2023-41715**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4417
Use of Hard-coded Credentials	17-Oct-2023	7.5	SonicOS Use of Hard-coded Password vulnerability in the 'dynHandleBuyToolbar' demo function. **CVE ID : CVE-2023-41713**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4418
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow vulnerability in the getBookmarkList.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39276**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4419
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication stack-based buffer overflow	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the sonicflow.csv and appflowsessions.csv URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39277**		
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi leads to a firewall crash. **CVE ID : CVE-2023-39278**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4421
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the getPacketReplayData.json URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-39279**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4422
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow vulnerability in the ssoStats-s.xml, ssoStats-s.wri URL endpoints leads to a firewall crash. **CVE ID : CVE-2023-39280**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the sonicwall.exp, prefs.exp URL endpoints lead to a firewall crash. **CVE ID : CVE-2023-41711**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4424
Out-of-bounds Write	17-Oct-2023	6.5	SonicOS post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN plainprefs.exp URL endpoint leads to a firewall crash. **CVE ID : CVE-2023-41712**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012	O-SON-SONI-281123/4425
Vendor: Synology					
Product: bc500_firmware					
Affected Version(s): * Up to (excluding) 1.0.5-0185					
Use of Externally-Controlled Format String	25-Oct-2023	9.8	A vulnerability regarding use of externally-controlled format string is found in the cgi component. This allows remote attackers to execute arbitrary code via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.5-0185 may be	https://www.synology.com/en-global/security/advisory/Synology_SA_23_11	O-SYN-BC50-281123/4426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected: BC500 and TC500. **CVE ID : CVE-2023-5746**		
Product: tc500_firmware					
Affected Version(s): * Up to (excluding) 1.0.5-0185					
Use of Externally-Controlled Format String	25-Oct-2023	9.8	A vulnerability regarding use of externally-controlled format string is found in the cgi component. This allows remote attackers to execute arbitrary code via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.5-0185 may be affected: BC500 and TC500. **CVE ID : CVE-2023-5746**	https://www.synology.com/en-global/security/advisory/Synology_SA_23_11	O-SYN-TC50-281123/4427
Vendor: Tenda					
Product: w18e_firmware					
Affected Version(s): 16.01.0.8\\(1576\\)					
Out-of-bounds Write	25-Oct-2023	9.8	Tenda W18E V16.01.0.8(1576) contains a stack overflow vulnerability via the portMirrorMirroredPorts parameter in the formSetNetCheckTools function.	N/A	O-TEN-W18E-281123/4428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46369		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	Tenda W18E V16.01.0.8(1576) has a command injection vulnerability via the hostName parameter in the formSetNetCheckTools function. **CVE ID : CVE-2023-46370**	N/A	O-TEN-W18E-281123/4429
Vendor: totolink					
Product: a3300r_firmware					
Affected Version(s): 17.0.0cu.557_b20221024					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	31-Oct-2023	9.8	TOTOLINK A3300R 17.0.0cu.557_B20221024 contains a command injection via the file_name parameter in the UploadFirmwareFile function. **CVE ID : CVE-2023-46976**	N/A	O-TOT-A330-281123/4430
Product: a3700r_firmware					
Affected Version(s): 9.1.2u.6165_20211012					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	An issue in TOTOLINK A3700R v.9.1.2u.6165_20211012 allows a remote attacker to execute arbitrary code via the FileName parameter of the UploadFirmwareFile function.	N/A	O-TOT-A370-281123/4431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46574		
Product: a7000r_firmware					
Affected Version(s): 9.1.0u.6115_b20201022					
Out-of-bounds Write	16-Oct-2023	9.8	TOTOLINK X5000R V9.1.0u.6118_B20201102 and TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the File parameter in the function UploadCustomModule. **CVE ID : CVE-2023-36947**	N/A	O-TOT-A700-281123/4432
Out-of-bounds Write	16-Oct-2023	9.8	TOTOLINK X5000R V9.1.0u.6118_B20201102 and TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the http_host parameter in the function loginAuth. **CVE ID : CVE-2023-36950**	N/A	O-TOT-A700-281123/4433
Out-of-bounds Write	16-Oct-2023	9.8	TOTOLINK X5000R V9.1.0u.6118_B20201102 and TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the	N/A	O-TOT-A700-281123/4434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lang parameter in the function setLanguageCfg. **CVE ID : CVE-2023-45984**		
Out-of-bounds Write	16-Oct-2023	7.5	TOTOLINK X5000R V9.1.0u.6118_B20201102 and TOTOLINK A7000R V9.1.0u.6115_B20201022 were discovered to contain a stack overflow in the function setParentalRules. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID : CVE-2023-45985**	N/A	O-TOT-A700-281123/4435
Product: cp300\+_firmware					
Affected Version(s): * Up to (including) 5.2cu.7594_b20200910					
Out-of-bounds Write	16-Oct-2023	9.8	TOTOLINK CP300+ <=V5.2cu.7594_B20200910 was discovered to contain a stack overflow via the File parameter in the function UploadCustomModule. **CVE ID : CVE-2023-36955**	N/A	O-TOT-CP30-281123/4436
Affected Version(s): 5.2cu.7594_b20200910					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Oct-2023	9.8	TOTOLINK CP300+ V5.2cu.7594_B20200910 was discovered to contain a stack overflow via the pingIp parameter in the function setDiagnosisCfg. **CVE ID : CVE-2023-36952**	N/A	O-TOT-CP30-281123/4437
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Oct-2023	9.8	TOTOLINK CP300+ V5.2cu.7594_B20200910 and before is vulnerable to command injection. **CVE ID : CVE-2023-36953**	N/A	O-TOT-CP30-281123/4438
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Oct-2023	9.8	TOTOLINK CP300+ V5.2cu.7594_B20200910 and before is vulnerable to command injection. **CVE ID : CVE-2023-36954**	N/A	O-TOT-CP30-281123/4439
Product: lr1200gb_firmware					
Affected Version(s): 9.1.0u.6619_b20230130					
Out-of-bounds Write	31-Oct-2023	9.8	TOTOLINK LR1200GB V9.1.0u.6619_B20230130 was discovered to contain a stack overflow via the password	N/A	O-TOT-LR12-281123/4440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter in the function loginAuth. **CVE ID : CVE-2023-46977**		
Product: nr1800x_firmware					
Affected Version(s): 9.1.0u.6279_b20210910					
Out-of-bounds Write	16-Oct-2023	9.8	TOTOLINK NR1800X V9.1.0u.6279_B20210910 was discovered to contain a stack overflow via the http_host parameter in the function loginAuth. **CVE ID : CVE-2023-36340**	N/A	O-TOT-NR18-281123/4441
Product: x2000r_firmware					
Affected Version(s): 1.0.0-b20230221.0948					
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formNtp. **CVE ID : CVE-2023-46540**	N/A	O-TOT-X200-281123/4442
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formIpv6Setup.	N/A	O-TOT-X200-281123/4443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46541		
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formMeshUploadConfig. **CVE ID : CVE-2023-46542**	N/A	O-TOT-X200-281123/4444
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formWlSiteSurvey. **CVE ID : CVE-2023-46543**	N/A	O-TOT-X200-281123/4445
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formWirelessTbl. **CVE ID : CVE-2023-46544**	N/A	O-TOT-X200-281123/4446
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack	N/A	O-TOT-X200-281123/4447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow via the function formWsc. **CVE ID : CVE-2023-46545**		
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formStats. **CVE ID : CVE-2023-46546**	N/A	O-TOT-X200-281123/4448
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formSysLog. **CVE ID : CVE-2023-46547**	N/A	O-TOT-X200-281123/4449
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formWlanRedirect. **CVE ID : CVE-2023-46548**	N/A	O-TOT-X200-281123/4450
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to	N/A	O-TOT-X200-281123/4451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a stack overflow via the function formSetLg. **CVE ID : CVE-2023-46549**		
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formMapDelDevice . **CVE ID : CVE-2023-46550**	N/A	O-TOT-X200-281123/4452
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formReflashClientTbl. **CVE ID : CVE-2023-46551**	N/A	O-TOT-X200-281123/4453
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formMultiAP. **CVE ID : CVE-2023-46552**	N/A	O-TOT-X200-281123/4454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formParentControl. **CVE ID : CVE-2023-46553**	N/A	O-TOT-X200-281123/4455
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formMapDel. **CVE ID : CVE-2023-46554**	N/A	O-TOT-X200-281123/4456
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formPortFw. **CVE ID : CVE-2023-46555**	N/A	O-TOT-X200-281123/4457
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formFilter.	N/A	O-TOT-X200-281123/4458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46556		
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formMultiAPVLAN. **CVE ID : CVE-2023-46557**	N/A	O-TOT-X200-281123/4459
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formMapDelDevice. **CVE ID : CVE-2023-46558**	N/A	O-TOT-X200-281123/4460
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formIPv6Addr. **CVE ID : CVE-2023-46559**	N/A	O-TOT-X200-281123/4461
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack	N/A	O-TOT-X200-281123/4462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow via the function formTcpipSetup. **CVE ID : CVE-2023-46560**		
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formDosCfg. **CVE ID : CVE-2023-46562**	N/A	O-TOT-X200-281123/4463
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formIpQoS. **CVE ID : CVE-2023-46563**	N/A	O-TOT-X200-281123/4464
Out-of-bounds Write	25-Oct-2023	9.8	TOTOLINK X2000R Gh v1.0.0-B20230221.0948. web was discovered to contain a stack overflow via the function formDMZ. **CVE ID : CVE-2023-46564**	N/A	O-TOT-X200-281123/4465
Product: x5000r_firmware					
Affected Version(s): 9.1.0u.6118_b20201102					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Oct-2023	9.8	TOTOLINK X5000R V9.1.0u.6118_B20201102 and TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the File parameter in the function UploadCustomModule. **CVE ID : CVE-2023-36947**	N/A	O-TOT-X500-281123/4466
Out-of-bounds Write	16-Oct-2023	9.8	TOTOLINK X5000R V9.1.0u.6118_B20201102 and TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the http_host parameter in the function loginAuth. **CVE ID : CVE-2023-36950**	N/A	O-TOT-X500-281123/4467
Out-of-bounds Write	16-Oct-2023	9.8	TOTOLINK X5000R V9.1.0u.6118_B20201102 and TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the lang parameter in the function setLanguageCfg.	N/A	O-TOT-X500-281123/4468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45984		
Out-of-bounds Write	16-Oct-2023	7.5	TOTOLINK X5000R V9.1.0u.6118_B20201102 and TOTOLINK A7000R V9.1.0u.6115_B20201022 were discovered to contain a stack overflow in the function setParentalRules. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request. **CVE ID : CVE-2023-45985**	N/A	O-TOT-X500-281123/4469
Product: x6000r_firmware					
Affected Version(s): 9.4.0cu.652_b20230116					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_ The 41DD80 function. **CVE ID : CVE-2023-46408**	N/A	O-TOT-X600-281123/4470
Improper Neutralization of Special Elements used in a Command ('Comman	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via	N/A	O-TOT-X600-281123/4471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			the sub_ 41CC04 function. **CVE ID : CVE-2023-46409**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_ The 416F60 function. **CVE ID : CVE-2023-46410**	N/A	O-TOT-X600-281123/4472
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_415258 function. **CVE ID : CVE-2023-46411**	N/A	O-TOT-X600-281123/4473
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a command execution vulnerability via the sub_41D998 function. **CVE ID : CVE-2023-46412**	N/A	O-TOT-X600-281123/4474
Improper Neutralization of Special	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to	N/A	O-TOT-X600-281123/4475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			contain a command execution vulnerability via the sub_4155DC function. **CVE ID : CVE-2023-46413**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_ 41D494 function. **CVE ID : CVE-2023-46414**	N/A	O-TOT-X600-281123/4476
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_41E588 function. **CVE ID : CVE-2023-46415**	N/A	O-TOT-X600-281123/4477
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_ The 41A414 function.	N/A	O-TOT-X600-281123/4478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46416		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_415498 function. **CVE ID : CVE-2023-46417**	N/A	O-TOT-X600-281123/4479
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_412688 function. **CVE ID : CVE-2023-46418**	N/A	O-TOT-X600-281123/4480
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_415730 function. **CVE ID : CVE-2023-46419**	N/A	O-TOT-X600-281123/4481
Improper Neutralization of Special	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to	N/A	O-TOT-X600-281123/4482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			contain a remote command execution (RCE) vulnerability via the sub_41590C function. **CVE ID : CVE-2023-46420**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_411D00 function. **CVE ID : CVE-2023-46421**	N/A	O-TOT-X600-281123/4483
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_411994 function. **CVE ID : CVE-2023-46422**	N/A	O-TOT-X600-281123/4484
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_417094 function.	N/A	O-TOT-X600-281123/4485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46423		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Oct-2023	9.8	TOTOLINK X6000R v9.4.0cu.652_B20230116 was discovered to contain a remote command execution (RCE) vulnerability via the sub_422BD4 function. **CVE ID : CVE-2023-46424**	N/A	O-TOT-X600-281123/4486
Affected Version(s): 9.4.0cu.852_b20230719					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	31-Oct-2023	9.8	TOTOLINK X6000R V9.4.0cu.852_B20230719 was discovered to contain a command injection vulnerability via the enable parameter in the setLedCfg function. **CVE ID : CVE-2023-46979**	N/A	O-TOT-X600-281123/4487
Missing Authentication for Critical Function	31-Oct-2023	7.5	TOTOLINK X6000R V9.4.0cu.852_B20230719 is vulnerable to Incorrect Access Control.Attackers can reset login password & WIFI passwords without authentication. **CVE ID : CVE-2023-46978**	N/A	O-TOT-X600-281123/4488
Vendor: Tp-link					
Product: tl-wdr7660_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.0.30					
Out-of-bounds Write	25-Oct-2023	9.8	TP-Link device TL-WDR7660 2.0.30 has a stack overflow vulnerability via the function upgradeInfoJsonToBin. **CVE ID : CVE-2023-46371**	N/A	O-TP--TL-W-281123/4489
Out-of-bounds Write	25-Oct-2023	9.8	TP-Link TL-WDR7660 2.0.30 has a stack overflow vulnerability via the function deviceInfoJsonToBincauses. **CVE ID : CVE-2023-46373**	N/A	O-TP--TL-W-281123/4490
Product: tl-wr886n_firmware					
Affected Version(s): 3.0.14					
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function uninstallPluginReqHandle. **CVE ID : CVE-2023-46520**	N/A	O-TP--TL-W-281123/4491
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was	N/A	O-TP--TL-W-281123/4492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a stack overflow via the function RegisterRegister. **CVE ID : CVE-2023-46521**		
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function deviceInfoRegister. **CVE ID : CVE-2023-46522**	N/A	O-TP--TL-W-281123/4493
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function upgradeInfoRegister. **CVE ID : CVE-2023-46523**	N/A	O-TP--TL-W-281123/4494
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function loginRegister.	N/A	O-TP--TL-W-281123/4495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46525		
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function resetCloudPwdRegister. **CVE ID : CVE-2023-46526**	N/A	O-TP--TL-W-281123/4496
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function bindRequestHandle. **CVE ID : CVE-2023-46527**	N/A	O-TP--TL-W-281123/4497
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function modifyAccPwdRegister. **CVE ID : CVE-2023-46534**	N/A	O-TP--TL-W-281123/4498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function getResetVeriRegister. **CVE ID : CVE-2023-46535**	N/A	O-TP--TL-W-281123/4499
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function chkRegVeriRegister. **CVE ID : CVE-2023-46536**	N/A	O-TP--TL-W-281123/4500
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function getRegVeriRegister. **CVE ID : CVE-2023-46537**	N/A	O-TP--TL-W-281123/4501
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_	N/A	O-TP--TL-W-281123/4502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			221115_Rel.56908n.bin was discovered to contain a stack overflow via the function chkResetVeriRegister. **CVE ID : CVE-2023-46538**		
Out-of-bounds Write	25-Oct-2023	9.8	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function registerRequestHandle. **CVE ID : CVE-2023-46539**	N/A	O-TP--TL-W-281123/4503
Vendor: viessmann					
Product: vitogate_300_firmware					
Affected Version(s): * Up to (including) 2.1.3.0					
Direct Request ('Forced Browsing')	23-Oct-2023	6.5	A vulnerability was found in Viessmann Vitogate 300 up to 2.1.3.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /cgi-bin/. The manipulation leads to direct request. The exploit has been disclosed to	N/A	O-VIE-VITO-281123/4504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. The identifier of this vulnerability is VDB-243140. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-5702**		
Vendor: Wago					
Product: compact_controller_100_firmware					
Affected Version(s): From (including) 19 Up to (including) 26					
Externally Controlled Reference to a Resource in Another Sphere	17-Oct-2023	2.7	On affected Wago products an remote attacker with administrative privileges can access files to which he has already access to through an undocumented local file inclusion. This access is logged in a different log file than expected. **CVE ID : CVE-2023-4089**	N/A	O-WAG-COMP-281123/4505
Product: edge_controller_firmware					
Affected Version(s): From (including) 18 Up to (including) 26					
Externally Controlled Reference to a Resource	17-Oct-2023	2.7	On affected Wago products an remote attacker with administrative	N/A	O-WAG-EDGE-281123/4506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
in Another Sphere			privileges can access files to which he has already access to through an undocumented local file inclusion. This access is logged in a different log file than expected. **CVE ID : CVE-2023-4089**		
Product: pfc100_firmware					
Affected Version(s): From (including) 16 Up to (including) 26					
Externally Controlled Reference to a Resource in Another Sphere	17-Oct-2023	2.7	On affected Wago products an remote attacker with administrative privileges can access files to which he has already access to through an undocumented local file inclusion. This access is logged in a different log file than expected. **CVE ID : CVE-2023-4089**	N/A	O-WAG-PFC1-281123/4507
Product: pfc200_firmware					
Affected Version(s): From (including) 16 Up to (including) 26					
Externally Controlled Reference to a Resource	17-Oct-2023	2.7	On affected Wago products an remote attacker with administrative privileges can	N/A	O-WAG-PFC2-281123/4508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
in Another Sphere			access files to which he has already access to through an undocumented local file inclusion. This access is logged in a different log file than expected. **CVE ID : CVE-2023-4089**		
Product: touch_panel_600_advanced_firmware					
Affected Version(s): From (including) 16 Up to (including) 26					
Externally Controlled Reference to a Resource in Another Sphere	17-Oct-2023	2.7	On affected Wago products an remote attacker with administrative privileges can access files to which he has already access to through an undocumented local file inclusion. This access is logged in a different log file than expected. **CVE ID : CVE-2023-4089**	N/A	O-WAG-TOUC-281123/4509
Product: touch_panel_600_marine_firmware					
Affected Version(s): From (including) 16 Up to (including) 26					
Externally Controlled Reference to a Resource in Another Sphere	17-Oct-2023	2.7	On affected Wago products an remote attacker with administrative privileges can access files to	N/A	O-WAG-TOUC-281123/4510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which he has already access to through an undocumented local file inclusion. This access is logged in a different log file than expected. **CVE ID : CVE-2023-4089**		
Product: touch_panel_600_standard_firmware					
Affected Version(s): From (including) 16 Up to (including) 26					
Externally Controlled Reference to a Resource in Another Sphere	17-Oct-2023	2.7	On affected Wago products an remote attacker with administrative privileges can access files to which he has already access to through an undocumented local file inclusion. This access is logged in a different log file than expected. **CVE ID : CVE-2023-4089**	N/A	O-WAG-TOUC-281123/4511
Vendor: weintek					
Product: cmt-fhd_firmware					
Affected Version(s): * Up to (excluding) 20210212					
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin command_wb.cgi contains a stack-based buffer	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT--281123/4512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-38584**		
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin codesys.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-43492**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT--281123/4513
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Oct-2023	8.8	In Weintek's cMT3000 HMI Web CGI device, an anonymous attacker can execute arbitrary commands after login to the device. **CVE ID : CVE-2023-40145**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT--281123/4514
Product: cmt-hdm_firmware					
Affected Version(s): * Up to (excluding) 20210206					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin command_wb.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-38584**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT--281123/4515
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin codesys.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-43492**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT--281123/4516
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Oct-2023	8.8	In Weintek's cMT3000 HMI Web CGI device, an anonymous attacker can execute arbitrary commands after login to the device.	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT--281123/4517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-40145		
Product: cmt3071_firmware					
Affected Version(s): * Up to (excluding) 20210220					
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin command_wb.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-38584**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT3-281123/4518
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin codesys.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-43492**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT3-281123/4519
Improper Neutralization of Special Elements used in an OS	19-Oct-2023	8.8	In Weintek's cMT3000 HMI Web CGI device, an anonymous attacker can execute arbitrary	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT3-281123/4520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			commands after login to the device. **CVE ID : CVE-2023-40145**		
Product: cmt3072_firmware					
Affected Version(s): * Up to (excluding) 20210220					
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin command_wb.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-38584**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT3-281123/4521
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin codesys.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-43492**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT3-281123/4522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Oct-2023	8.8	In Weintek's cMT3000 HMI Web CGI device, an anonymous attacker can execute arbitrary commands after login to the device. **CVE ID : CVE-2023-40145**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT3-281123/4523
Product: cmt3090_firmware					
Affected Version(s): * Up to (excluding) 20210220					
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin command_wb.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-38584**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT3-281123/4524
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin codesys.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT3-281123/4525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass login authentication. **CVE ID : CVE-2023-43492**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Oct-2023	8.8	In Weintek's cMT3000 HMI Web CGI device, an anonymous attacker can execute arbitrary commands after login to the device. **CVE ID : CVE-2023-40145**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT3-281123/4526
Product: cmt3103_firmware					
Affected Version(s): * Up to (excluding) 20210220					
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin command_wb.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-38584**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT3-281123/4527
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin codesys.cgi contains a stack-based buffer overflow, which	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT3-281123/4528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-43492**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Oct-2023	8.8	In Weintek's cMT3000 HMI Web CGI device, an anonymous attacker can execute arbitrary commands after login to the device. **CVE ID : CVE-2023-40145**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT3-281123/4529
Product: cmt3151_firmware					
Affected Version(s): * Up to (excluding) 20210220					
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin command_wb.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-38584**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT3-281123/4530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Oct-2023	9.8	In Weintek's cMT3000 HMI Web CGI device, the cgi-bin codesys.cgi contains a stack-based buffer overflow, which could allow an anonymous attacker to hijack control flow and bypass login authentication. **CVE ID : CVE-2023-43492**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT3-281123/4531
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Oct-2023	8.8	In Weintek's cMT3000 HMI Web CGI device, an anonymous attacker can execute arbitrary commands after login to the device. **CVE ID : CVE-2023-40145**	https://dl.weintek.com/public/Document/TEC/TEC23005E_cMT_Web_Security_Update.pdf	O-WEI-CMT3-281123/4532
Vendor: Yealink					
Product: sip-t19p-e2_firmware					
Affected Version(s): 53.84.0.15					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Oct-2023	8.8	An issue in YeaLinkSIP-T19P-E2 v.53.84.0.15 allows a remote privileged attacker to execute arbitrary code via a crafted request the ping function of the diagnostic component.	N/A	O-YEA-SIP--281123/4533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43959		
Vendor: zephyrproject					
Product: zephyr					
Affected Version(s): * Up to (including) 3.4.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	25-Oct-2023	8.8	Potential buffer overflows in the Bluetooth subsystem due to asserts being disabled in /subsys/bluetooth /host/hci_core.c **CVE ID : CVE-2023-5753**	https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-hmpr-px56-rvww	O-ZEP-ZEPH-281123/4534
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	26-Oct-2023	7.8	Potential buffer overflow vulnerability at the following location in the Zephyr STM32 Crypto driver **CVE ID : CVE-2023-5139**	https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-rhrc-pcxp-4453	O-ZEP-ZEPH-281123/4535
Vendor: zioncom					
Product: a7000r_firmware					
Affected Version(s): 4.1cu.4154					
N/A	27-Oct-2023	9.8	An issue in ZIONCOM (Hong Kong) Technology Limited A7000R v.4.1cu.4154 allows an attacker to execute arbitrary code via the cig-bin/cstecgi.cgi to the	N/A	O-ZIO-A700-281123/4536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			settings/setPasswordCfg function. **CVE ID : CVE-2023-46510**		
Vendor: zpesystems					
Product: nodegrid_os					
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.0.18					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	28-Oct-2023	8.8	ZPE Systems, Inc Nodegrid OS v5.0.0 to v5.0.17, v5.2.0 to v5.2.19, v5.4.0 to v5.4.16, v5.6.0 to v5.6.13, v5.8.0 to v5.8.10, and v5.10.0 to v5.10.3 was discovered to contain a command injection vulnerability via the endpoint /v1/system/toolkit/files/. **CVE ID : CVE-2023-43322**	https://psirt.zpesystems.com/portal/en/kb/articles/security-advisory-zpe-ng-2023-001-12-10-2023	O-ZPE-NODE-281123/4537
Affected Version(s): From (including) 5.10.0 Up to (excluding) 5.10.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	28-Oct-2023	8.8	ZPE Systems, Inc Nodegrid OS v5.0.0 to v5.0.17, v5.2.0 to v5.2.19, v5.4.0 to v5.4.16, v5.6.0 to v5.6.13, v5.8.0 to v5.8.10, and v5.10.0 to v5.10.3 was discovered to contain a command injection vulnerability via the endpoint /v1/system/toolkit/files/.	https://psirt.zpesystems.com/portal/en/kb/articles/security-advisory-zpe-ng-2023-001-12-10-2023	O-ZPE-NODE-281123/4538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43322		
Affected Version(s): From (including) 5.2.0 Up to (excluding) 5.2.20					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	28-Oct-2023	8.8	ZPE Systems, Inc Nodegrid OS v5.0.0 to v5.0.17, v5.2.0 to v5.2.19, v5.4.0 to v5.4.16, v5.6.0 to v5.6.13, v5.8.0 to v5.8.10, and v5.10.0 to v5.10.3 was discovered to contain a command injection vulnerability via the endpoint /v1/system/toolkit/files/. **CVE ID : CVE-2023-43322**	https://psirt.zpesystems.com/portal/en/kb/articles/security-advisory-zpe-ng-2023-001-12-10-2023	O-ZPE-NODE-281123/4539
Affected Version(s): From (including) 5.4.0 Up to (excluding) 5.4.17					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	28-Oct-2023	8.8	ZPE Systems, Inc Nodegrid OS v5.0.0 to v5.0.17, v5.2.0 to v5.2.19, v5.4.0 to v5.4.16, v5.6.0 to v5.6.13, v5.8.0 to v5.8.10, and v5.10.0 to v5.10.3 was discovered to contain a command injection vulnerability via the endpoint /v1/system/toolkit/files/. **CVE ID : CVE-2023-43322**	https://psirt.zpesystems.com/portal/en/kb/articles/security-advisory-zpe-ng-2023-001-12-10-2023	O-ZPE-NODE-281123/4540
Affected Version(s): From (including) 5.6.0 Up to (excluding) 5.6.14					
Improper Neutralizat	28-Oct-2023	8.8	ZPE Systems, Inc Nodegrid OS v5.0.0	https://psirt.zpesystems.com/p	O-ZPE-NODE-281123/4541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			to v5.0.17, v5.2.0 to v5.2.19, v5.4.0 to v5.4.16, v5.6.0 to v5.6.13, v5.8.0 to v5.8.10, and v5.10.0 to v5.10.3 was discovered to contain a command injection vulnerability via the endpoint /v1/system/toolkit/files/. **CVE ID : CVE-2023-43322**	ortal/en/kb/articles/security-advisory-zpe-ng-2023-001-12-10-2023	
Affected Version(s): From (including) 5.8.0 Up to (excluding) 5.8.11					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	28-Oct-2023	8.8	ZPE Systems, Inc Nodegrid OS v5.0.0 to v5.0.17, v5.2.0 to v5.2.19, v5.4.0 to v5.4.16, v5.6.0 to v5.6.13, v5.8.0 to v5.8.10, and v5.10.0 to v5.10.3 was discovered to contain a command injection vulnerability via the endpoint /v1/system/toolkit/files/. **CVE ID : CVE-2023-43322**	https://psirt.zpesystems.com/portal/en/kb/articles/security-advisory-zpe-ng-2023-001-12-10-2023	O-ZPE-NODE-281123/4542