تمت مشاركة هذه المعلومة بإشارة مشاركة ***أبيض*** حيث يسمح بتبادلها أو نشرها من خلال القنوات العامة.

Please note that this notification/advisory has been tagged as TLP ***WHITE*** where information can be shared or published on any public forums.

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ٢٨ أبريل إلى ٥ ماي. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- عالي جدًا: النتيجة الأساسية لـCVSS 9.0-10.0
- عالي: النتيجة الأساسية لـCVSS 7.0-8.9
- متوسط: النتيجة الأساسية لـCVSS 4.0-6.9
- منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 28th of April to 5th of May. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

- Critical: CVSS base score of 9.0-10.0
- High: CVSS base score of 7.0-8.9
- Medium: CVSS base score 4.0-6.9
- Low: CVSS base score 0.0-3.9

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2024-25050	IBM	IBM i 7.2, 7.3, 7.4, 7.5 and IBM Rational Development Studio for i 7.2, 7.3, 7.4, 7.5 networking and compiler infrastructure could allow a local user to gain elevated privileges due to an unqualified library call. A malicious actor could cause user-controlled code to run with administrator privileges. IBM X-Force ID: 283242.	2024-04-28	8.4	High
CVE-2022-48655	Linux	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Harden accesses to the reset domains Accessing reset domains descriptors by the index upon the SCMI drivers requests through the SCMI reset operations interface can potentially lead to out-of-bound violations if the SCMI driver misbehave. Add an internal consistency check before any such domains descriptors accesses.	2024-04-28	7.8	High
CVE-2022-48658	Linux	In the Linux kernel, the following vulnerability has been resolved: mm: slub: fix flush_cpu_slab()/__free_slab() invocations in task context. Commit 5a836bf6b09f ("mm: slub: move flush_cpu_slab() invocations __free_slab() invocations out of IRQ context") moved all flush_cpu_slab() invocations to the global workqueue to avoid a problem related with deactivate_slab()/__free_slab() being called from an IRQ context on PREEMPT_RT kernels. When the flush_all_cpu_locked() function is called from a task context it may happen that a workqueue with WQ_MEM_RECLAIM bit set ends up flushing the global workqueue, this will cause a dependency issue. workqueue: WQ_MEM_RECLAIM nvme-delete-wq:nvme_delete_ctrl_work [nvme_core] is flushing !WQ_MEM_RECLAIM events:flush_cpu_slab WARNING: CPU: 37 PID: 410 at kernel/workqueue.c:2637 check_flush_dependency+0x10a/0x120 Workqueue: nvme-delete-wq nvme_delete_ctrl_work [nvme_core] RIP: 0010:check_flush_dependency+0x10a/0x120[453.262125] Call Trace: __flush_work.isra.0+0xbf/0x220 ? __queue_work+0x1dc/0x420	2024-04-28	7.8	High

		flush_all_cpus_locked+0xfb/0x120 __kmem_cache_shutdown+0x2b/0x320 kmem_cache_destroy+0x49/0x100 bioset_exit+0x143/0x190 blk_release_queue+0xb9/0x100 kobject_cleanup+0x37/0x130 nvme_fc_ctrl_free+0xc6/0x150 [nvme_fc] nvme_free_ctrl+0x1ac/0x2b0 [nvme_core] Fix this bug by creating a workqueue for the flush operation with the WQ_MEM_RECLAIM bit set.			
CVE-2022-48662	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/i915/gem: Really move i915_gem_context.link under ref protection i915_perf assumes that it can use the i915_gem_context reference to protect its i915->gem.contexts.list iteration. However, this requires that we do not remove the context from the list until after we drop the final reference and release the struct. If, as currently, we remove the context from the list during context_close(), the link.next pointer may be poisoned while we are holding the context reference and cause a GPF: [4070.573157] i915 0000:00:02.0: [drm:i915_perf_open_ioctl [i915]] filtering on ctx_id=0x1fffff ctx_id_mask=0x1fffff [4070.574881] general protection fault, probably for non-canonical address 0xdead000000000100: 0000 [#1] PREEMPT SMP [4070.574897] CPU: 1 PID: 284392 Comm: amd_performance Tainted: G E 5.17.9 #180 [4070.574903] Hardware name: Intel Corporation NUC7i5BNK/NUC7i5BNB, BIOS BNKBL357.86A.0052.2017.0918.1346 09/18/2017 [4070.574907] RIP: 0010:oa_configure_all_contexts.isra.0+0x222/0x350 [i915] [4070.574982] Code: 08 e8 32 6e 10 e1 4d 8b 6d 50 b8 ff ff ff ff 49 83 ed 50 f0 41 0f c1 04 24 83 f8 01 0f 84 e3 00 00 00 85 c0 0f 8e fa 00 00 00 <49> 8b 45 50 48 8d 70 b0 49 8d 45 50 48 39 44 24 10 0f 85 34 fe ff [4070.574990] RSP: 0018:ffffc90002077b78 EFLAGS: 00010202 [4070.574995] RAX: 0000000000000002 RBX: 0000000000000002 RCX: 0000000000000000 [4070.575000] RDX: 0000000000000001 RSI: ffffc90002077b20 RDI: ffff88810ddc7c68 [4070.575004] RBP: 0000000000000001 R08: ffff888103242648 R09: fffffffffffffffc [4070.575008] R10: ffffffff82c50bc0 R11: 0000000000025c80 R12: ffff888101bf1860 [4070.575012] R13: dead0000000000b0 R14: ffffc90002077c04 R15: ffff88810be5cabc [4070.575016] FS: 00007f1ed50c0780(0000) GS:ffff88885ec80000(0000) knlGS:0000000000000000 [4070.575021] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [4070.575025] CR2: 00007f1ed5590280 CR3: 000000010ef6f005 CR4: 00000000003706e0 [4070.575029] Call Trace: [4070.575033] <TASK> [4070.575037] lrc_configure_all_contexts+0x13e/0x150 [i915] [4070.575103] gen8_enable_metric_set+0x4d/0x90 [i915] [4070.575164] i915_perf_open_ioctl+0xbc0/0x1500 [i915] [4070.575224] ? asm_common_interrupt+0x1e/0x40 [4070.575232] ? i915_oa_init_reg_state+0x110/0x110 [i915] [4070.575290] drm_ioctl_kernel+0x85/0x110 [4070.575296] ? update_load_avg+0x5f/0x5e0 [4070.575302] drm_ioctl+0x1d3/0x370 [4070.575307] ? i915_oa_init_reg_state+0x110/0x110 [i915] [4070.575382] ? gen8_gt_irq_handler+0x46/0x130 [i915] [4070.575445] __x64_sys_ioctl+0x3c4/0x8d0 [4070.575451] ? __do_softirq+0xaa/0x1d2 [4070.575456] do_syscall_64+0x35/0x80 [4070.575461] entry_SYSCALL_64_after_hwframe+0x44/0xae [4070.575467] RIP: 0033:0x7f1ed5c10397 [4070.575471] Code: 3c 1c e8 1c ff ff ff 85 c0 79 87 49 c7 c4 ff ff ff ff 5b 5d 4c 89 e0 41 5c c3 66 0f 1f 84 00 00 00 00 00 b8 10 00 00	2024-04-28	7.8	High

		00 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d a9 da 0d 00 f7 d8 64 89 01 48 [4070.575478] RSP: 002b:00007ffd65c8d7a8 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 [4070.575484] RAX: ffffffffffffffda RBX: 0000000000000006 RCX: 00007f1ed5c10397 [4070.575488] RDX: 00007ffd65c8d7c0 RSI: 0000000040106476 RDI: 0000000000000006 [4070.575492] RBP: 00005620972f9c60 R08: 000000000000000a R09: 0000000000000005 [4070.575496] R10: 000000000000000d R11: 0000000000000246 R12: 000000000000000a [4070.575500] R13: 000000000000000d R14: 0000000000000000 R15: 00007ffd65c8d7c0 [4070.575505] </TASK> [4070.575507] Modules linked in: nls_ascii(E) nls_cp437(E) vfat(E) fat(E) i915(E) x86_pkg_temp_thermal(E) intel_powerclamp(E) crct10dif_pclmul(E) crc32_pclmul(E) crc32c_intel(E) aesni_intel(E) crypto_simd(E) intel_gtt(E) cryptd(E) ttm(E) rapl(E) intel_cstate(E) drm_kms_helper(E) cfbfillrect(E) syscopyarea(E) cfbimgblt(E) intel_uncore(E) sysfillrect(E) mei_me(E) sysimgblt(E) i2c_i801(E) fb_sys_fops(E) mei(E) intel_pch_thermal(E) i2c_smbus ---truncated---			
CVE-2022-48659	Linux	In the Linux kernel, the following vulnerability has been resolved: mm/slub: fix to return errno if kmalloc() fails In create_unique_id(), kmalloc(, GFP_KERNEL) can fail due to out-of-memory, if it fails, return errno correctly rather than triggering panic via BUG_ON(); kernel BUG at mm/slub.c:5893! Internal error: Oops - BUG: 0 [#1] PREEMPT SMP Call trace: sysfs_slab_add+0x258/0x260 mm/slub.c:5973 __kmem_cache_create+0x60/0x118 mm/slub.c:4899 create_cache mm/slab_common.c:229 [inline] kmem_cache_create_usercopy+0x19c/0x31c mm/slab_common.c:335 kmem_cache_create+0x1c/0x28 mm/slab_common.c:390 f2fs_kmem_cache_create fs/f2fs/f2fs.h:2766 [inline] f2fs_init_xattr_caches+0x78/0xb4 fs/f2fs/xattr.c:808 f2fs_fill_super+0x1050/0x1e0c fs/f2fs/super.c:4149 mount_bdev+0x1b8/0x210 fs/super.c:1400 f2fs_mount+0x44/0x58 fs/f2fs/super.c:4512 legacy_get_tree+0x30/0x74 fs/fs_context.c:610 vfs_get_tree+0x40/0x140 fs/super.c:1530 do_new_mount+0x1dc/0x4e4 fs/namespace.c:3040 path_mount+0x358/0x914 fs/namespace.c:3370 do_mount fs/namespace.c:3383 [inline] __do_sys_mount fs/namespace.c:3591 [inline] __se_sys_mount fs/namespace.c:3568 [inline] __arm64_sys_mount+0x2f8/0x408 fs/namespace.c:3568	2024-04-28	5.5	Medium
CVE-2022-48660	Linux	In the Linux kernel, the following vulnerability has been resolved: gpiolib: cdev: Set lineevent_state::irq after IRQ register successfully When running gpio test on nxp-ls1028 platform with below command gpiomon --num-events=3 --rising-edge gpiochip1 25 There will be a warning trace as below: Call trace: free_irq+0x204/0x360 lineevent_free+0x64/0x70 gpio_ioctl+0x598/0x6a0 __arm64_sys_ioctl+0xb4/0x100 invoke_syscall+0x5c/0x130 ..... el0t_64_sync+0x1a0/0x1a4 The reason of this issue is that calling request_threaded_irq() function failed, and then lineevent_free() is invoked to release the resource. Since the lineevent_state::irq was already set, so the subsequent invocation of free_irq() would trigger the above warning call trace. To fix this issue, set the lineevent_state::irq after the IRQ register successfully.	2024-04-28	5.5	Medium
CVE-2022-48661	Linux	In the Linux kernel, the following vulnerability has been resolved: gpio: mockup: Fix potential resource leakage when register a chip	2024-04-28	5.5	Medium

		If creation of software node fails, the locally allocated string array is left unfreed. Free it on error path.			
CVE-2024-0840	Grandstream	The Grandstream UCM Series IP PBX before firmware version 1.0.20.52 is affected by a parameter injection vulnerability in the HTTP interface. A remote and authenticated attacker can execute arbitrary code by sending a crafted HTTP request. Authentication may be possible using a default user and password. Affected models are the UCM6202, UCM6204, UCM6208, and UCM6510.	2024-04-29	8.8	High
CVE-2024-28961	Dell	Dell OpenManage Enterprise, versions 4.0.0 and 4.0.1, contains a sensitive information disclosure vulnerability. A local low privileged malicious user could potentially exploit this vulnerability to obtain credentials leading to unauthorized access with elevated privileges. This could lead to further attacks, thus Dell recommends customers to upgrade at the earliest opportunity.	2024-04-29	6.3	Medium
CVE-2023-38002	IBM	IBM Storage Scale 5.1.0.0 through 5.1.9.2 could allow an authenticated user to steal or manipulate an active session to gain access to the system. IBM X-Force ID: 260208.	2024-04-30	5	Medium
CVE-2024-20376	Cisco	A vulnerability in the web-based management interface of Cisco IP Phone firmware could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a DoS condition. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to cause the affected device to reload.	2024-05-01	7.5	High
CVE-2024-20378	Cisco	A vulnerability in the web-based management interface of Cisco IP Phone firmware could allow an unauthenticated, remote attacker to retrieve sensitive information from an affected device. This vulnerability is due to a lack of authentication for specific endpoints of the web-based management interface on an affected device. An attacker could exploit this vulnerability by connecting to the affected device. A successful exploit could allow the attacker to gain unauthorized access to the device, enabling the recording of user credentials and traffic to and from the affected device, including VoIP calls that could be replayed.	2024-05-01	7.5	High
CVE-2024-25015	IBM	IBM MQ 9.2 LTS, 9.3 LTS, and 9.3 CD Internet Pass-Thru could allow a remote user to cause a denial of service by sending HTTP requests that would consume all available resources. IBM X-Force ID: 281278.	2024-05-01	7.5	High
CVE-2024-29011	SonicWall	Use of hard-coded password in the GMS ECM endpoint leading to authentication bypass vulnerability. This issue affects GMS: 9.3.4 and earlier versions.	2024-05-01	7.5	High
CVE-2024-29010	SonicWall	The XML document processed in the GMS ECM URL endpoint is vulnerable to XML external entity (XXE) injection, potentially resulting in the disclosure of sensitive information. This issue affects GMS: 9.3.4 and earlier versions.	2024-05-01	7.1	High
CVE-2024-28764	IBM	IBM WebSphere Automation 1.7.0 could allow an attacker with privileged access to the network to conduct a CSV injection. An attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 285623.	2024-05-01	6.5	Medium
CVE-2022-38386	IBM	IBM Cloud Pak for Security (CP4S) 1.10.0.0 through 1.10.11.0 and IBM QRadar Suite for Software 1.10.12.0 through 1.10.19.0 does not set the SameSite attribute for sensitive cookies which could allow an attacker to obtain sensitive information using man-in-the-middle techniques. IBM X-Force ID: 233778.	2024-05-01	5.9	Medium
CVE-2024-20357	Cisco	A vulnerability in the XML service of Cisco IP Phone firmware could allow an unauthenticated, remote attacker to initiate phone calls on an affected device. This vulnerability exists because bounds-checking does not occur while parsing XML requests. An attacker could exploit this vulnerability by sending a crafted XML request to an affected device. A successful exploit could allow the attacker to initiate calls or play sounds on the device.	2024-05-01	5.9	Medium
CVE-2024-28978	Dell	Dell OpenManage Enterprise, versions 3.10 and 4.0, contains an Improper Access Control vulnerability. A high privileged remote attacker could potentially exploit this vulnerability, leading to unauthorized access to resources.	2024-05-01	5.2	Medium
CVE-2024-28979	Dell	Dell OpenManage Enterprise, versions prior to 4.1.0, contains an XSS injection vulnerability in UI. A high privileged local attacker	2024-05-01	5.1	Medium

		could potentially exploit this vulnerability, leading to JavaScript injection.			
CVE-2024-28775	IBM	IBM WebSphere Automation 1.7.0 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: 285648.	2024-05-01	4.4	Medium
CVE-2024-25047	IBM	IBM Cognos Analytics 11.2.0 through 11.2.4 and 12.0.0 through 12.0.2 is vulnerable to injection attacks in application logging by not sanitizing user provided data. This could lead to further attacks against the system. IBM X-Force ID: 282956.	2024-05-02	8.6	High
CVE-2024-30301	Adobe	Acrobat Reader versions 20.005.30539, 23.008.20470 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-02	7.8	High
CVE-2024-30303	Adobe	Acrobat Reader versions 20.005.30539, 23.008.20470 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-02	7.8	High
CVE-2024-30304	Adobe	Acrobat Reader versions 20.005.30539, 23.008.20470 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-02	7.8	High
CVE-2024-30305	Adobe	Acrobat Reader versions 20.005.30539, 23.008.20470 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-02	7.8	High
CVE-2024-30306	Adobe	Acrobat Reader versions 20.005.30539, 23.008.20470 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-02	7.8	High
CVE-2023-51631	D-Link	D-Link DIR-X3260 prog.cgi SetUsersSettings Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-size stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21675.	2024-05-02	6.8	Medium
CVE-2024-30302	Adobe	Acrobat Reader versions 20.005.30539, 23.008.20470 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-05-02	5.5	Medium
CVE-2023-47727	IBM	IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 and IBM QRadar Suite Software 1.10.12.0 through 1.10.20.0 could allow an authenticated user to modify dashboard parameters due to improper input validation. IBM X-Force ID: 272089.	2024-05-02	4.3	Medium
CVE-2023-27359	TP-Link	TP-Link AX1800 hotplugd Firewall Rule Race Condition Vulnerability. This vulnerability allows remote attackers to gain access to LAN-side services on affected installations of TP-Link Archer AX21 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the hotplugd daemon. The issue results from firewall rule handling that allows an attacker access to resources that should be available to the LAN interface only. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the root user. Was ZDI-CAN-19664.	2024-05-03	9.8	Critical
CVE-2023-32165	D-Link	D-Link D-View TftpReceiveFileHandler Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of D-Link D-View. Authentication is not required to exploit this vulnerability. The specific flaw exists within the TftpReceiveFileHandler class.	2024-05-03	9.8	Critical

		The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-19497.			
CVE-2023-32169	D-Link	D-Link D-View Use of Hard-coded Cryptographic Key Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected installations of D-Link D-View. Authentication is not required to exploit this vulnerability. The specific flaw exists within the TokenUtils class. The issue results from a hard-coded cryptographic key. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-19659.	2024-05-03	9.8	Critical
CVE-2023-38096	NETGEAR	NETGEAR ProSAFE Network Management System MyHandlerInterceptor Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected installations of NETGEAR ProSAFE Network Management System. Authentication is not required to exploit this vulnerability. The specific flaw exists within the MyHandlerInterceptor class. The issue results from improper implementation of the authentication mechanism. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-19718.	2024-05-03	9.8	Critical
CVE-2023-40493	LG	LG Simple Editor copySessionFolder Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the copySessionFolder command. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-19920.	2024-05-03	9.8	Critical
CVE-2023-40497	LG	LG Simple Editor saveXml Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the saveXml command implemented in the makeDetailContent method. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-19924.	2024-05-03	9.8	Critical
CVE-2023-40498	LG	LG Simple Editor cp Command Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the cp command implemented in the makeDetailContent method. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-19925.	2024-05-03	9.8	Critical
CVE-2023-40500	LG	LG Simple Editor copyContent Exposed Dangerous Function Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the copyContent command. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-19944.	2024-05-03	9.8	Critical
CVE-2023-40501	LG	LG Simple Editor copyContent Exposed Dangerous Function Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the copyContent command. The issue results from an exposed dangerous function. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-19945.	2024-05-03	9.8	Critical
CVE-2023-40504	LG	LG Simple Editor readVideoInfo Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability.	2024-05-03	9.8	Critical

		The specific flaw exists within the readVideoInfo method. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-19953.			
CVE-2023-40505	LG	LG Simple Editor createThumbnailByMovie Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the createThumbnailByMovie method. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-19978.	2024-05-03	9.8	Critical
CVE-2023-42115	Exim	Exim AUTH Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Exim. Authentication is not required to exploit this vulnerability. The specific flaw exists within the smtp service, which listens on TCP port 25 by default. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of a buffer. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-17434.	2024-05-03	9.8	Critical
CVE-2023-44411	D-Link	D-Link D-View InstallApplication Use of Hard-coded Credentials Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected installations of D-Link D-View. Authentication is not required to exploit this vulnerability. The specific flaw exists within the InstallApplication class. The class contains a hard-coded password for the remotely reachable database. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-19553.	2024-05-03	9.8	Critical
CVE-2023-44414	D-Link	D-Link D-View coreservice_action_script Exposed Dangerous Function Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of D-Link D-View. Authentication is not required to exploit this vulnerability. The specific flaw exists within the coreservice_action_script action. The issue results from the exposure of a dangerous function. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-19573.	2024-05-03	9.8	Critical
CVE-2023-27332	TP-Link	TP-Link Archer AX21 tdpServer Logging Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link Archer AX21 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the logging functionality of the tdpServer program, which listens on UDP port 20002. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19898.	2024-05-03	8.8	High
CVE-2023-27346	TP-Link	TP-Link AX1800 Firmware Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link AX1800 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the parsing of firmware images. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19703.	2024-05-03	8.8	High
CVE-2023-27358	NETGEAR	NETGEAR RAX30 SOAP Request SQL Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR RAX30 routers. Authentication is not required to exploit this vulnerability.The specific flaw exists within the handling of specific SOAP requests. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this in conjunction with other	2024-05-03	8.8	High

		vulnerabilities to execute arbitrary code in the context of the service account. Was ZDI-CAN-19754.			
CVE-2023-27368	NETGEAR	NETGEAR RAX30 soap_serverd Stack-based Buffer Overflow Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR RAX30 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the soap_serverd binary. When parsing SOAP message headers, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-19839.	2024-05-03	8.8	High
CVE-2023-27369	NETGEAR	NETGEAR RAX30 soap_serverd Stack-based Buffer Overflow Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR RAX30. Authentication is not required to exploit this vulnerability. The specific flaw exists within the soap_serverd binary. When parsing the request headers, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-19840.	2024-05-03	8.8	High
CVE-2023-32136	D-Link	D-Link DAP-1360 webproc var:menu Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1360 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling requests to the /cgi-bin/webproc endpoint. When parsing the var:menu parameter, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18414.	2024-05-03	8.8	High
CVE-2023-32139	D-Link	D-Link DAP-1360 webproc Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1360 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling requests to the /cgi-bin/webproc endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18417.	2024-05-03	8.8	High
CVE-2023-32141	D-Link	D-Link DAP-1360 webproc WEB_DisplayPage Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1360 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of requests to the /cgi-bin/webproc endpoint. When parsing the getpage and errorpage parameters, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18419.	2024-05-03	8.8	High
CVE-2023-32142	D-Link	D-Link DAP-1360 webproc var:page Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1360 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of requests to the /cgi-bin/webproc endpoint. When parsing the var:page parameter, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18422.	2024-05-03	8.8	High
CVE-2023-32143	D-Link	D-Link DAP-1360 webupg UPGCGI_CheckAuth Numeric Truncation Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1360 routers. Authentication is not required to exploit this vulnerability.	2024-05-03	8.8	High

		The specific flaw exists within the handling of requests to the /cgi-bin/webupg endpoint. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18423.			
CVE-2023-32144	D-Link	D-Link DAP-1360 webproc COMM_MakeCustomMsg Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1360 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of requests to the /cgi-bin/webproc endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18454.	2024-05-03	8.8	High
CVE-2023-32145	D-Link	D-Link DAP-1360 Hardcoded Credentials Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DAP-1360 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of login requests to the web-based user interface. The firmware contains hard-coded default credentials. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-18455.	2024-05-03	8.8	High
CVE-2023-32146	D-Link	D-Link DAP-1360 Multiple Parameters Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1360 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the /cgi-bin/webproc endpoint. When parsing the errorpage and nextpage parameters, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18746.	2024-05-03	8.8	High
CVE-2023-32149	D-Link	D-Link DIR-2640 prog.cgi Request Handling Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-2640 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the web management interface, which listens on TCP port 80 by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19546.	2024-05-03	8.8	High
CVE-2023-32168	D-Link	D-Link D-View showUser Improper Authorization Privilege Escalation Vulnerability. This vulnerability allows remote attackers to escalate privileges on affected installations of D-Link D-View. Authentication is required to exploit this vulnerability. The specific flaw exists within the showUser method. The issue results from the lack of proper authorization before accessing a privileged endpoint. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from the user. Was ZDI-CAN-19534.	2024-05-03	8.8	High
CVE-2023-34274	D-Link	D-Link DIR-2150 LoginPassword Incorrect Implementation of Authentication Algorithm Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-2150 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SOAP API interface, which listens on TCP port 80 by default. A crafted login request can cause authentication to succeed without providing proper credentials. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-20552.	2024-05-03	8.8	High
CVE-2023-34282	D-Link	D-Link DIR-2150 HNAP Incorrect Implementation of Authentication Algorithm Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-2150 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SOAP API interface, which listens	2024-05-03	8.8	High

		on TCP port 80 by default. A crafted authentication header can cause authentication to succeed without providing proper credentials. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-20910.			
CVE-2023-34285	NETGEAR	NETGEAR RAX30 cmsCli_authenticate Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR RAX30 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within a shared library used by the telnetd service, which listens on TCP port 23 by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19918.	2024-05-03	8.8	High
CVE-2023-35717	TP-Link	TP-Link Tapo C210 Password Recovery Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of TP-Link Tapo C210 IP cameras. Authentication is not required to exploit this vulnerability. The specific flaw exists within the password recovery mechanism. The issue results from reliance upon the secrecy of the password derivation algorithm when generating a recovery password. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-20484.	2024-05-03	8.8	High
CVE-2023-35718	D-Link	D-Link DAP-2622 DDP Change ID Password Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20061.	2024-05-03	8.8	High
CVE-2023-35722	NETGEAR	NETGEAR RAX30 UPnP Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR RAX30 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of UPnP port mapping requests. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20429.	2024-05-03	8.8	High
CVE-2023-35723	D-Link	D-Link DIR-X3260 prog.cgi SOAPAction Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the SOAPAction request header provided to the prog.cgi endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20983.	2024-05-03	8.8	High
CVE-2023-35724	D-Link	D-Link DAP-2622 Telnet CLI Use of Hardcoded Credentials Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the CLI service, which listens on TCP port 23. The server program contains hard-coded credentials. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-20050.	2024-05-03	8.8	High
CVE-2023-35725	D-Link	D-Link DAP-2622 DDP User Verification Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An	2024-05-03	8.8	High

		attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20052.			
CVE-2023-35726	D-Link	D-Link DAP-2622 DDP User Verification Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20053.	2024-05-03	8.8	High
CVE-2023-35727	D-Link	D-Link DAP-2622 DDP Reboot Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20054.	2024-05-03	8.8	High
CVE-2023-35728	D-Link	D-Link DAP-2622 DDP Reboot Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20055.	2024-05-03	8.8	High
CVE-2023-35729	D-Link	D-Link DAP-2622 DDP Reset Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20056.	2024-05-03	8.8	High
CVE-2023-35730	D-Link	D-Link DAP-2622 DDP Reset Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20057.	2024-05-03	8.8	High
CVE-2023-35731	D-Link	D-Link DAP-2622 DDP Reset Factory Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20058.	2024-05-03	8.8	High
CVE-2023-35732	D-Link	D-Link DAP-2622 DDP Reset Factory Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20059.	2024-05-03	8.8	High

CVE-2023-35733	D-Link	D-Link DAP-2622 DDP Change ID Password Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20060.	2024-05-03	8.8	High
CVE-2023-35735	D-Link	D-Link DAP-2622 DDP Change ID Password New Username Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20062.	2024-05-03	8.8	High
CVE-2023-35736	D-Link	D-Link DAP-2622 DDP Change ID Password New Password Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20063.	2024-05-03	8.8	High
CVE-2023-35737	D-Link	D-Link DAP-2622 DDP Configuration Backup Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20064.	2024-05-03	8.8	High
CVE-2023-35738	D-Link	D-Link DAP-2622 DDP Configuration Backup Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20065.	2024-05-03	8.8	High
CVE-2023-35739	D-Link	D-Link DAP-2622 DDP Configuration Backup Server IPv6 Address Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20066.	2024-05-03	8.8	High
CVE-2023-35740	D-Link	D-Link DAP-2622 DDP Configuration Backup Server Address Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20067.	2024-05-03	8.8	High
CVE-2023-35741	D-Link	D-Link DAP-2622 DDP Configuration Backup Filename Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute	2024-05-03	8.8	High

		arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20068.			
CVE-2023-35742	D-Link	D-Link DAP-2622 DDP Configuration Restore Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20069.	2024-05-03	8.8	High
CVE-2023-35743	D-Link	D-Link DAP-2622 DDP Configuration Restore Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. . Was ZDI-CAN-20070.	2024-05-03	8.8	High
CVE-2023-35744	D-Link	D-Link DAP-2622 DDP Configuration Restore Server IPv6 Address Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20071.	2024-05-03	8.8	High
CVE-2023-35745	D-Link	D-Link DAP-2622 DDP Configuration Restore Filename Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20073.	2024-05-03	8.8	High
CVE-2023-35746	D-Link	D-Link DAP-2622 DDP Firmware Upgrade Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20074.	2024-05-03	8.8	High
CVE-2023-35747	D-Link	D-Link DAP-2622 DDP Firmware Upgrade Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20075.	2024-05-03	8.8	High
CVE-2023-35751	D-Link	D-Link DAP-2622 DDP Set AG Profile Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability.	2024-05-03	8.8	High

		The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20079.			
CVE-2023-35752	D-Link	D-Link DAP-2622 DDP Set AG Profile Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20080.	2024-05-03	8.8	High
CVE-2023-35753	D-Link	D-Link DAP-2622 DDP Set AG Profile UUID Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20081.	2024-05-03	8.8	High
CVE-2023-35754	D-Link	D-Link DAP-2622 DDP Set AG Profile NMS URL Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20082.	2024-05-03	8.8	High
CVE-2023-35755	D-Link	D-Link DAP-2622 DDP Set Date-Time Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability.The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20083.	2024-05-03	8.8	High
CVE-2023-35756	D-Link	D-Link DAP-2622 DDP Set Date-Time Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20084.	2024-05-03	8.8	High
CVE-2023-37310	D-Link	D-Link DAP-2622 DDP Set Device Info Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20087.	2024-05-03	8.8	High
CVE-2023-37311	D-Link	D-Link DAP-2622 DDP Set Device Info Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An	2024-05-03	8.8	High

		attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20088.			
CVE-2023-37312	D-Link	D-Link DAP-2622 DDP Set Device Info Device Name Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20089.	2024-05-03	8.8	High
CVE-2023-37313	D-Link	D-Link DAP-2622 DDP Set IPv4 Address Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20090.	2024-05-03	8.8	High
CVE-2023-37314	D-Link	D-Link DAP-2622 DDP Set IPv6 Address Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20092.	2024-05-03	8.8	High
CVE-2023-37315	D-Link	D-Link DAP-2622 DDP Set IPv6 Address Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20093.	2024-05-03	8.8	High
CVE-2023-37316	D-Link	D-Link DAP-2622 DDP Set IPv6 Address Default Gateway Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20094.	2024-05-03	8.8	High
CVE-2023-37317	D-Link	D-Link DAP-2622 DDP Set IPv6 Address Primary DNS Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20095.	2024-05-03	8.8	High
CVE-2023-37318	D-Link	D-Link DAP-2622 DDP Set IPv6 Address Secondary DNS Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20096.	2024-05-03	8.8	High

CVE-2023-37319	D-Link	D-Link DAP-2622 DDP Set IPv6 Address Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20097.	2024-05-03	8.8	High
CVE-2023-37320	D-Link	D-Link DAP-2622 DDP Set SSID List SSID Name Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20098.	2024-05-03	8.8	High
CVE-2023-37321	D-Link	D-Link DAP-2622 DDP Set SSID List RADIUS Secret Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20099.	2024-05-03	8.8	High
CVE-2023-37322	D-Link	D-Link DAP-2622 DDP Set SSID List RADIUS Server Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20100.	2024-05-03	8.8	High
CVE-2023-37323	D-Link	D-Link DAP-2622 DDP Set SSID List PSK Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20101.	2024-05-03	8.8	High
CVE-2023-37324	D-Link	D-Link DAP-2622 DDP Set Wireless Info Auth Username Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20102.	2024-05-03	8.8	High
CVE-2023-37326	D-Link	D-Link DAP-2622 DDP Set Wireless Info Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20103.	2024-05-03	8.8	High
CVE-2023-38095	NETGEAR	NETGEAR ProSAFE Network Management System MFileUploadController Unrestricted File Upload Remote Code Execution Vulnerability. This vulnerability allows remote attackers	2024-05-03	8.8	High

		to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the MFileUploadController class. The issue results from the lack of proper validation of user-supplied data, which can allow the upload of arbitrary files. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-19717.			
CVE-2023-38098	NETGEAR	NETGEAR ProSAFE Network Management System UpLoadServlet Unrestricted File Upload Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the UpLoadServlet class. The issue results from the lack of proper validation of user-supplied data, which can allow the upload of arbitrary files. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-19720.	2024-05-03	8.8	High
CVE-2023-38099	NETGEAR	NETGEAR ProSAFE Network Management System getNodesByTopologyMapSearch SQL Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the getNodesByTopologyMapSearch function. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-19723.	2024-05-03	8.8	High
CVE-2023-38100	NETGEAR	NETGEAR ProSAFE Network Management System clearAlertByIds SQL Injection Privilege Escalation Vulnerability. This vulnerability allows remote attackers to escalate privileges on affected installations of NETGEAR ProSAFE Network Management System. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the clearAlertByIds function. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from the user. Was ZDI-CAN-19724.	2024-05-03	8.8	High
CVE-2023-38102	NETGEAR	NETGEAR ProSAFE Network Management System createUser Missing Authorization Privilege Escalation Vulnerability. This vulnerability allows remote attackers to escalate privileges on affected installations of NETGEAR ProSAFE Network Management System. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the createUser function. The issue results from the lack of authorization prior to allowing access to functionality. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from the user. Was ZDI-CAN-19726.	2024-05-03	8.8	High
CVE-2023-40479	NETGEAR	NETGEAR RAX30 UPnP Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR RAX30 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the UPnP service. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19704.	2024-05-03	8.8	High
CVE-2023-40480	NETGEAR	NETGEAR RAX30 DHCP Server Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR RAX30 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DHCP server. The issue results from the lack of proper validation of a user-supplied string before	2024-05-03	8.8	High

		using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19705.			
CVE-2023-41183	NETGEAR	NETGEAR Orbi 760 SOAP API Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR Orbi 760 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the SOAP API. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-20524.	2024-05-03	8.8	High
CVE-2023-41187	D-Link	D-Link DAP-1325 HNAP Missing Authentication Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the HNAP interface. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18807.	2024-05-03	8.8	High
CVE-2023-41188	D-Link	D-Link DAP-1325 HNAP SetAPLanSettings DeviceName Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of a request parameter provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18808.	2024-05-03	8.8	High
CVE-2023-41189	D-Link	D-Link DAP-1325 HNAP SetAPLanSettings Gateway Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of a request parameter provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18809.	2024-05-03	8.8	High
CVE-2023-41190	D-Link	D-Link DAP-1325 HNAP SetAPLanSettings IPAddr Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of a request parameter provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18810.	2024-05-03	8.8	High
CVE-2023-41191	D-Link	D-Link DAP-1325 HNAP SetAPLanSettings Mode Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of a request parameter provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18811.	2024-05-03	8.8	High
CVE-2023-41192	D-Link	D-Link DAP-1325 HNAP SetAPLanSettings PrimaryDNS Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of a request parameter provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18812.	2024-05-03	8.8	High

CVE-2023-41193	D-Link	D-Link DAP-1325 HNAP SetAPLanSettings SecondaryDNS Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of a request parameter provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18813.	2024-05-03	8.8	High
CVE-2023-41194	D-Link	D-Link DAP-1325 HNAP SetAPLanSettings SubnetMask Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of a request parameter provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18814.	2024-05-03	8.8	High
CVE-2023-41195	D-Link	D-Link DAP-1325 HNAP SetHostIPv6Settings IPv6Mode Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of a request parameter provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18815.	2024-05-03	8.8	High
CVE-2023-41196	D-Link	D-Link DAP-1325 HNAP SetHostIPv6StaticSettings StaticAddress Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of a request parameter provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18816.	2024-05-03	8.8	High
CVE-2023-41197	D-Link	D-Link DAP-1325 HNAP SetHostIPv6StaticSettings StaticDefaultGateway Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of a request parameter provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18817.	2024-05-03	8.8	High
CVE-2023-41198	D-Link	D-Link DAP-1325 HNAP SetHostIPv6StaticSettings StaticDNS1 Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of a request parameter provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18818.	2024-05-03	8.8	High
CVE-2023-41199	D-Link	D-Link DAP-1325 HNAP SetHostIPv6StaticSettings StaticDNS2 Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of a request parameter provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18819.	2024-05-03	8.8	High
CVE-2023-41200	D-Link	D-Link DAP-1325 HNAP SetHostIPv6StaticSettings StaticPrefixLength Command Injection Remote Code Execution	2024-05-03	8.8	High

		Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of a request parameter provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18820.			
CVE-2023-41201	D-Link	D-Link DAP-1325 HNAP SetSetupWizardStatus Enabled Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of a request parameter provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18821.	2024-05-03	8.8	High
CVE-2023-41202	D-Link	D-Link DAP-1325 SetAPLanSettings Mode Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of XML data provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18828.	2024-05-03	8.8	High
CVE-2023-41203	D-Link	D-Link DAP-1325 SetAPLanSettings PrimaryDNS Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of XML data provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18829.	2024-05-03	8.8	High
CVE-2023-41204	D-Link	D-Link DAP-1325 SetAPLanSettings SecondaryDNS Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of XML data provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18830.	2024-05-03	8.8	High
CVE-2023-41205	D-Link	D-Link DAP-1325 SetAPLanSettings SubnetMask Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of XML data provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18831.	2024-05-03	8.8	High
CVE-2023-41206	D-Link	D-Link DAP-1325 SetHostIPv6Settings IPv6Mode Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of XML data provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can	2024-05-03	8.8	High

		leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18832.			
CVE-2023-41207	D-Link	D-Link DAP-1325 SetHostIPv6StaticSettings StaticAddress Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of XML data provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18833.	2024-05-03	8.8	High
CVE-2023-41208	D-Link	D-Link DAP-1325 SetHostIPv6StaticSettings StaticDefaultGateway Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability.The specific flaw exists within the handling of XML data provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18834.	2024-05-03	8.8	High
CVE-2023-41209	D-Link	D-Link DAP-1325 SetHostIPv6StaticSettings StaticDNS1 Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of XML data provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18835.	2024-05-03	8.8	High
CVE-2023-41210	D-Link	D-Link DAP-1325 SetHostIPv6StaticSettings StaticDNS2 Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of XML data provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18836.	2024-05-03	8.8	High
CVE-2023-41211	D-Link	D-Link DAP-1325 SetHostIPv6StaticSettings StaticPrefixLength Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of XML data provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18837.	2024-05-03	8.8	High
CVE-2023-41212	D-Link	D-Link DAP-1325 SetTriggerAPValidate Key Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of XML data provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18839.	2024-05-03	8.8	High
CVE-2023-41213	D-Link	D-Link DAP-1325 setDhcpAssignRangeUpdate lan_ipaddr Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of XML data provided	2024-05-03	8.8	High

		to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18840.			
CVE-2023-41214	D-Link	D-Link DAP-1325 setDhcpAssignRangeUpdate lan_ipaddr Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of XML data provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18841.	2024-05-03	8.8	High
CVE-2023-41215	D-Link	D-Link DAP-2622 DDP Set Date-Time Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20086.	2024-05-03	8.8	High
CVE-2023-41229	D-Link	D-Link DIR-3040 HTTP Request Processing Referer Heap-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-3040 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21671.	2024-05-03	8.8	High
CVE-2023-44403	D-Link	D-Link DAP-1325 HNAP SetWLanRadioSettings Channel Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of a request parameter provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18822.	2024-05-03	8.8	High
CVE-2023-44404	D-Link	D-Link DAP-1325 get_value_from_app Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of XML data provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18823.	2024-05-03	8.8	High
CVE-2023-44405	D-Link	D-Link DAP-1325 get_value_of_key Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of XML data provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18824.	2024-05-03	8.8	High
CVE-2023-44406	D-Link	D-Link DAP-1325 SetAPLanSettings DeviceName Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability.	2024-05-03	8.8	High

		The specific flaw exists within the handling of XML data provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18825.			
CVE-2023-44407	D-Link	D-Link DAP-1325 SetAPLanSettings Gateway Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of XML data provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18826.	2024-05-03	8.8	High
CVE-2023-44408	D-Link	D-Link DAP-1325 SetAPLanSettings IPAddr Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of XML data provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18827.	2024-05-03	8.8	High
CVE-2023-44409	D-Link	D-Link DAP-1325 SetSetupWizardStatus Enabled Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of XML data provided to the HNAP1 SOAP endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18838.	2024-05-03	8.8	High
CVE-2023-44410	D-Link	D-Link D-View showUsers Improper Authorization Privilege Escalation Vulnerability. This vulnerability allows remote attackers to escalate privileges on affected installations of D-Link D-View. Authentication is required to exploit this vulnerability. The specific flaw exists within the showUsers method. The issue results from the lack of proper authorization before accessing a privileged endpoint. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from the user. Was ZDI-CAN-19535.	2024-05-03	8.8	High
CVE-2023-44417	D-Link	D-Link DAP-2622 DDP Set IPv4 Address Auth Password Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20091.	2024-05-03	8.8	High
CVE-2023-44418	D-Link	D-Link DIR-X3260 Prog.cgi Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver. The issue results from the lack of proper validation of the length an user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20727.	2024-05-03	8.8	High
CVE-2023-44419	D-Link	D-Link DIR-X3260 Prog.cgi Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Authentication is not	2024-05-03	8.8	High

		required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver. The issue results from the lack of proper validation of the length an user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20774.			
CVE-2023-44420	D-Link	D-Link DIR-X3260 prog.cgi Incorrect Implementation of Authentication Algorithm Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-X3260 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the prog.cgi executable. The issue results from an incorrect implementation of the authentication algorithm. An attacker can leverage this vulnerability to bypass authentication on the device. Was ZDI-CAN-21100.	2024-05-03	8.8	High
CVE-2023-44445	NETGEAR	NETGEAR CAX30 SSO Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR CAX30 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the sso binary. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19058.	2024-05-03	8.8	High
CVE-2023-44449	NETGEAR	NETGEAR ProSAFE Network Management System clearAlertByIds SQL Injection Privilege Escalation Vulnerability. This vulnerability allows remote attackers to escalate privileges on affected installations of NETGEAR ProSAFE Network Management System. Authentication is required to exploit this vulnerability. The specific flaw exists within the clearAlertByIds function. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from the user. Was ZDI-CAN-21875.	2024-05-03	8.8	High
CVE-2023-44450	NETGEAR	NETGEAR ProSAFE Network Management System getNodesByTopologyMapSearch SQL Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System. Authentication is required to exploit this vulnerability. The specific flaw exists within the getNodesByTopologyMapSearch function. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-21858.	2024-05-03	8.8	High
CVE-2023-50198	D-Link	D-Link G416 cfgsave Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 wireless routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21286.	2024-05-03	8.8	High
CVE-2023-50199	D-Link	D-Link G416 httpd Missing Authentication for Critical Function Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link G416 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to gain access to critical functions on the device. Was ZDI-CAN-21287.	2024-05-03	8.8	High
CVE-2023-50200	D-Link	D-Link G416 cfgsave backusb Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 routers. Authentication is not required to exploit this vulnerability.	2024-05-03	8.8	High

		The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21288.			
CVE-2023-50201	D-Link	D-Link G416 cfgsave upusb Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21289.	2024-05-03	8.8	High
CVE-2023-50202	D-Link	D-Link G416 flupl pythonmodules Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 wireless routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21295.	2024-05-03	8.8	High
CVE-2023-50203	D-Link	D-Link G416 nodered chmod Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21296.	2024-05-03	8.8	High
CVE-2023-50204	D-Link	D-Link G416 flupl pythonapp Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 wireless routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21297.	2024-05-03	8.8	High
CVE-2023-50205	D-Link	D-Link G416 awsfile chmod Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21298.	2024-05-03	8.8	High
CVE-2023-50206	D-Link	D-Link G416 flupl query_type edit Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21299.	2024-05-03	8.8	High
CVE-2023-50207	D-Link	D-Link G416 flupl filename Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An	2024-05-03	8.8	High

		attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21300.			
CVE-2023-50208	D-Link	D-Link G416 ovpncfg Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21441.	2024-05-03	8.8	High
CVE-2023-50209	D-Link	D-Link G416 cfgsave Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 wireless routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21442.	2024-05-03	8.8	High
CVE-2023-50210	D-Link	D-Link G416 httpd API-AUTH Digest Processing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21662.	2024-05-03	8.8	High
CVE-2023-50211	D-Link	D-Link G416 httpd API-AUTH Timestamp Processing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21663.	2024-05-03	8.8	High
CVE-2023-50213	D-Link	D-Link G416 nodered File Handling Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21807.	2024-05-03	8.8	High
CVE-2023-50214	D-Link	D-Link G416 nodered tar File Handling Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21808.	2024-05-03	8.8	High
CVE-2023-50215	D-Link	D-Link G416 nodered gz File Handling Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21809.	2024-05-03	8.8	High

CVE-2023-50216	D-Link	D-Link G416 awsfile tar File Handling Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21810.	2024-05-03	8.8	High
CVE-2023-50217	D-Link	D-Link G416 awsfile rm Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21811.	2024-05-03	8.8	High
CVE-2023-51624	D-Link	D-Link DCS-8300LHV2 RTSP ValidateAuthorizationHeader Nonce Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DCS-8300LHV2 IP cameras. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the Authorization header by the RTSP server, which listens on TCP port 554. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20072.	2024-05-03	8.8	High
CVE-2023-51626	D-Link	D-Link DCS-8300LHV2 RTSP ValidateAuthorizationHeader Username Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DCS-8300LHV2 IP cameras. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the Authorization header by the RTSP server, which listens on TCP port 554. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21320.	2024-05-03	8.8	High
CVE-2023-37407	IBM	IBM Aspera Orchestrator 4.0.1 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 260116.	2024-05-03	8.8	High
CVE-2023-40492	LG	LG Simple Editor deleteCheckSession Directory Traversal Arbitrary File Deletion Vulnerability. This vulnerability allows remote attackers to delete arbitrary files on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the deleteCheckSession method. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to delete files in the context of SYSTEM. Was ZDI-CAN-19919.	2024-05-03	8.2	High
CVE-2023-40494	LG	LG Simple Editor deleteFolder Directory Traversal Arbitrary File Deletion Vulnerability. This vulnerability allows remote attackers to delete arbitrary files on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability.The specific flaw exists within the deleteFolder method. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to delete files in the context of SYSTEM. Was ZDI-CAN-19921.	2024-05-03	8.2	High
CVE-2023-40499	LG	LG Simple Editor mkdir Directory Traversal Arbitrary File Deletion Vulnerability. This vulnerability allows remote attackers to delete arbitrary files on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the mkdir command implemented in the makeDetailContent method. The issue results from the lack of proper validation of a user-supplied path prior to using it in file	2024-05-03	8.2	High

		operations. An attacker can leverage this vulnerability to delete files in the context of SYSTEM. Was ZDI-CAN-19926.			
CVE-2023-40502	LG	LG Simple Editor cropImage Directory Traversal Arbitrary File Deletion Vulnerability. This vulnerability allows remote attackers to delete arbitrary files on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the cropImage command. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to delete files in the context of SYSTEM. Was ZDI-CAN-19951.	2024-05-03	8.2	High
CVE-2023-40508	LG	LG Simple Editor putCanvasDB Directory Traversal Arbitrary File Deletion Vulnerability. This vulnerability allows remote attackers to delete arbitrary files on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the putCanvasDB method. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to delete files in the context of SYSTEM. Was ZDI-CAN-20010.	2024-05-03	8.2	High
CVE-2023-40509	LG	LG Simple Editor deleteCanvas Directory Traversal Arbitrary File Deletion Vulnerability. This vulnerability allows remote attackers to delete arbitrary files on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the deleteCanvas method. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to delete files in the context of SYSTEM. Was ZDI-CAN-20011.	2024-05-03	8.2	High
CVE-2023-44412	D-Link	D-Link D-View addDv7Probe XML External Entity Processing Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of D-Link D-View. Authentication is not required to exploit this vulnerability. The specific flaw exists within the addDv7Probe function. Due to the improper restriction of XML External Entity (XXE) references, a crafted document specifying a URI causes the XML parser to access the URI and embed the contents back into the XML document for further processing. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-19571.	2024-05-03	8.2	High
CVE-2023-32166	D-Link	D-Link D-View uploadFile Directory Traversal Arbitrary File Creation Vulnerability. This vulnerability allows remote attackers to create arbitrary files on affected installations of D-Link D-View. Authentication is required to exploit this vulnerability. The specific flaw exists within the uploadFile function. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to create files in the context of SYSTEM. Was ZDI-CAN-19527.	2024-05-03	8.1	High
CVE-2023-35721	NETGEAR	NETGEAR Multiple Routers curl_post Improper Certificate Validation Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to compromise the integrity of downloaded information on affected installations of multiple NETGEAR routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the update functionality, which operates over HTTPS. The issue results from the lack of proper validation of the certificate presented by the server. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-19981.	2024-05-03	8.1	High
CVE-2023-42116	Exim	Exim SMTP Challenge Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Exim. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of NTLM challenge requests. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-17515.	2024-05-03	8.1	High
CVE-2023-42117	Exim	Exim Improper Neutralization of Special Elements Remote Code Execution Vulnerability. This vulnerability allows remote attackers	2024-05-03	8.1	High

		to execute arbitrary code on affected installations of Exim. Authentication is not required to exploit this vulnerability. The specific flaw exists within the smtp service, which listens on TCP port 25 by default. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-17554.			
CVE-2023-27367	NETGEAR	NETGEAR RAX30 libcms_cli Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR RAX30 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the libcms_cli module. The issue results from the lack of proper validation of a user-supplied command before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19838.	2024-05-03	8	High
CVE-2023-40478	NETGEAR	NETGEAR RAX30 Telnet CLI passwd Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR RAX30 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the telnet CLI service, which listens on TCP port 23. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20009.	2024-05-03	8	High
CVE-2023-44421	D-Link	D-Link DIR-X3260 SetTriggerPPPoEValidate Username Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the prog.cgi program, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21101.	2024-05-03	8	High
CVE-2023-44422	D-Link	D-Link DIR-X3260 SetSysEmailSettings EmailFrom Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the prog.cgi program, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21102.	2024-05-03	8	High
CVE-2023-44423	D-Link	D-Link DIR-X3260 SetTriggerPPPoEValidate Password Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the prog.cgi program, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21157.	2024-05-03	8	High
CVE-2023-44424	D-Link	D-Link DIR-X3260 SetSysEmailSettings EmailTo Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed.	2024-05-03	8	High

		The specific flaw exists within prog.cgi, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21158.			
CVE-2023-44425	D-Link	D-Link DIR-X3260 SetSysEmailSettings AccountName Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within prog.cgi, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21159.	2024-05-03	8	High
CVE-2023-44426	D-Link	D-Link DIR-X3260 SetSysEmailSettings AccountPassword Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within prog.cgi, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21160.	2024-05-03	8	High
CVE-2023-44427	D-Link	D-Link DIR-X3260 SetSysEmailSettings SMTPServerAddress Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within prog.cgi, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21222.	2024-05-03	8	High
CVE-2023-50231	NETGEAR	NETGEAR ProSAFE Network Management System saveNodeLabel Cross-Site Scripting Privilege Escalation Vulnerability. This vulnerability allows remote attackers to escalate privileges on affected installations of NETGEAR ProSAFE Network Management System. Minimal user interaction is required to exploit this vulnerability. The specific flaw exists within the saveNodeLabel method. The issue results from the lack of proper validation of user-supplied data, which can lead to the injection of an arbitrary script. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from the user. Was ZDI-CAN-21838.	2024-05-03	8	High
CVE-2023-51625	D-Link	D-Link DCS-8300LHV2 ONVIF SetSystemDateAndTime Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DCS-8300LHV2 IP cameras. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the implementation of the ONVIF API, which listens on TCP port 80. When parsing the sch:TZ XML element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21319.	2024-05-03	8	High
CVE-2023-51627	D-Link	D-Link DCS-8300LHV2 ONVIF Duration Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DCS-8300LHV2 IP cameras. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the parsing of Duration XML elements. The issue results from the lack of proper validation of	2024-05-03	8	High

		the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21321.			
CVE-2023-51628	D-Link	D-Link DCS-8300LHV2 ONVIF SetHostName Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DCS-8300LHV2 IP cameras. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of the SetHostName ONVIF call. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21322.	2024-05-03	8	High
CVE-2023-40516	LG	LG Simple Editor Incorrect Permission Assignment Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of LG Simple Editor. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the product installer. The product sets incorrect permissions on folders. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-20327.	2024-05-03	7.8	High
CVE-2023-42099	Intel	Intel Driver & Support Assistant Link Following Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Intel Driver & Support Assistant. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the DSA Service. By creating a symbolic link, an attacker can abuse the service to delete a file. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-21846.	2024-05-03	7.8	High
CVE-2023-50197	Intel	Intel Driver & Support Assistant Link Following Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Intel Driver & Support Assistant. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the DSA Service. By creating a symbolic link, an attacker can abuse the service to write a file. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-21845.	2024-05-03	7.8	High
CVE-2023-27360	NETGEAR	NETGEAR RAX30 lighttpd Misconfiguration Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR RAX30. Authentication is not required to exploit this vulnerability. The specific flaw exists within the configuration of the lighttpd HTTP server. The issue results from allowing execution of files from untrusted sources. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19398.	2024-05-03	7.5	High
CVE-2023-32138	D-Link	D-Link DAP-1360 webproc Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1360 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of requests to the /cgi-bin/webproc endpoint. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18416.	2024-05-03	7.5	High
CVE-2023-32140	D-Link	D-Link DAP-1360 webproc var:sys_Token Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1360 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling requests to the /cgi-bin/webproc endpoint. When parsing the var:sys_Token	2024-05-03	7.5	High

		parameter, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-18418.			
CVE-2023-32154	Mikrotik	Mikrotik RouterOS RADVD Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Mikrotik RouterOS. Authentication is not required to exploit this vulnerability. The specific flaw exists within the Router Advertisement Daemon. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19797.	2024-05-03	7.5	High
CVE-2023-32164	D-Link	D-Link D-View TftpSendFileThread Directory Traversal Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of D-Link D-View. Authentication is not required to exploit this vulnerability. The specific flaw exists within the TftpSendFileThread class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-19496.	2024-05-03	7.5	High
CVE-2023-39471	TP-Link	TP-Link TL-WR841N ated_tp Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link TL-WR841N routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the ated_tp service. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21825.	2024-05-03	7.5	High
CVE-2023-40495	LG	LG Simple Editor copyTemplateAll Directory Traversal Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the copyTemplateAll method. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-19922.	2024-05-03	7.5	High
CVE-2023-40496	LG	LG Simple Editor copyStickerContent Directory Traversal Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the copyStickerContent command. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-19923.	2024-05-03	7.5	High
CVE-2023-40503	LG	LG Simple Editor saveXmlFile XML External Entity Processing Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the saveXmlFile method. Due to the improper restriction of XML External Entity (XXE) references, a crafted document specifying a URI causes the XML parser to access the URI and embed the contents back into the XML document for further processing. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-19952.	2024-05-03	7.5	High
CVE-2023-40506	LG	LG Simple Editor copyContent XML External Entity Processing Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the copyContent command. Due to the improper restriction of XML External Entity (XXE) references, a crafted document specifying a	2024-05-03	7.5	High

		URI causes the XML parser to access the URI and embed the contents back into the XML document for further processing. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-20005.			
CVE-2023-40507	LG	LG Simple Editor copyContent XML External Entity Processing Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the copyContent command. Due to the improper restriction of XML External Entity (XXE) references, a crafted document specifying a URI causes the XML parser to access the URI and embed the contents back into the XML document for further processing. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-20006.	2024-05-03	7.5	High
CVE-2023-40510	LG	LG Simple Editor getServerSetting Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the getServerSetting method. The issue results from the exposure of plaintext credentials. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-20012.	2024-05-03	7.5	High
CVE-2023-40511	LG	LG Simple Editor checkServer Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the checkServer method. The issue results from the exposure of plaintext credentials. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-20013.	2024-05-03	7.5	High
CVE-2023-40515	LG	LG Simple Editor joinAddUser Improper Input Validation Denial-of-Service Vulnerability. This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of LG Simple Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the joinAddUser method. The issue results from improper input validation. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-20048.	2024-05-03	7.5	High
CVE-2023-40517	LG	LG SuperSign Media Editor ContentRestController getObject Directory Traversal Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of LG SuperSign Media Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the getObject method implemented in the ContentRestController class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-20328.	2024-05-03	7.5	High
CVE-2023-41230	D-Link	D-Link DIR-3040 HTTP Request Processing Referer Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-3040 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed size stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21674.	2024-05-03	7.5	High
CVE-2023-42118	Exim	Exim libspf2 Integer Underflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Exim libspf2. Authentication is not required to exploit this vulnerability. The specific flaw exists within the parsing of SPF macros. When parsing SPF macros, the process does not properly validate user-supplied data, which can result in an integer underflow before writing to memory. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-17578.	2024-05-03	7.5	High

CVE-2023-35750	D-Link	D-Link DAP-2622 DDP Get SSID List WPA PSK Information Disclosure Vulnerability. This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of D-Link DAP-2622 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DDP service. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-20078.	2024-05-03	7.4	High
CVE-2023-38097	NETGEAR	NETGEAR ProSAFE Network Management System BkreProcessThread Exposed Dangerous Function Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the BkreProcessThread class. The issue results from an exposed dangerous function. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. . Was ZDI-CAN-19719.	2024-05-03	7.2	High
CVE-2023-38101	NETGEAR	NETGEAR ProSAFE Network Management System SettingConfigController Exposed Dangerous Function Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the SettingConfigController class. The issue results from an exposed dangerous function. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-19725.	2024-05-03	7.2	High
CVE-2023-41182	NETGEAR	NETGEAR ProSAFE Network Management System ZipUtils Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the ZipUtils class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-19716.	2024-05-03	7.2	High
CVE-2023-41217	D-Link	D-Link DIR-3040 prog.cgi SetQuickVPNSettings Password Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-3040 routers. Authentication is required to exploit this vulnerability.The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21617.	2024-05-03	7.1	High
CVE-2023-42114	Exim	Exim NTLM Challenge Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of Exim. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of NTLM challenge requests. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure. An attacker can leverage this vulnerability to disclose information in the context of the service account. Was ZDI-CAN-17433.	2024-05-03	3.7	Low
CVE-2023-23474	IBM	IBM Cognos Controller 10.4.1, 10.4.2, and 11.0.0 could allow a remote attacker to obtain sensitive information when a stack trace is returned in the browser. IBM X-Force ID: 245403.	2024-05-03	3.7	Low
CVE-2023-42119	Exim	Exim dnsdb Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of Exim. Authentication is not required to exploit this vulnerability. The specific flaw exists within the smtp service, which listens on	2024-05-03	3.1	Low

		TCP port 25 by default. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the service account. Was ZDI-CAN-17643.			
CVE-2023-27333	TP-Link	TP-Link Archer AX21 tmpServer Command 0x422 Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link Archer AX21 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the handling of command 0x422 provided to the tmpServer service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19905.	2024-05-03	6.8	Medium
CVE-2023-27356	NETGEAR	NETGEAR RAX30 logCtrl Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR RAX30 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the logCtrl action. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19825.	2024-05-03	6.8	Medium
CVE-2023-27361	NETGEAR	NETGEAR RAX30 rex_cgi JSON Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR RAX30 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the handling of JSON data. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19355.	2024-05-03	6.8	Medium
CVE-2023-32147	D-Link	D-Link DIR-2640 LocalIPAddress Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-2640 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of the LocalIPAddress parameter provided to the HNAP1 endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19544.	2024-05-03	6.8	Medium
CVE-2023-32150	D-Link	D-Link DIR-2640 PrefixLen Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-2640 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of the PrefixLen parameter provided to the HNAP1 endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19547.	2024-05-03	6.8	Medium
CVE-2023-32151	D-Link	D-Link DIR-2640 DestNetwork Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-2640 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of the DestNetwork parameter provided to the HNAP1 endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19548.	2024-05-03	6.8	Medium

CVE-2023-32153	D-Link	D-Link DIR-2640 EmailFrom Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-2640 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of the EmailFrom parameter provided to the HNAP1 endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19550.	2024-05-03	6.8	Medium
CVE-2023-34275	D-Link	D-Link DIR-2150 SetNTPServerSettings Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-2150 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the SOAP API interface, which listens on TCP port 80 by default. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20553.	2024-05-03	6.8	Medium
CVE-2023-34276	D-Link	D-Link DIR-2150 SetTriggerPPPoEValidate Username Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-2150 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the SOAP API interface, which listens on TCP port 80 by default. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20554.	2024-05-03	6.8	Medium
CVE-2023-34277	D-Link	D-Link DIR-2150 SetSysEmailSettings AccountName Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-2150 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the SOAP API interface, which listens on TCP port 80 by default. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20555.	2024-05-03	6.8	Medium
CVE-2023-34278	D-Link	D-Link DIR-2150 SetSysEmailSettings EmailFrom Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-2150 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the SOAP API interface, which listens on TCP port 80 by default. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20556.	2024-05-03	6.8	Medium
CVE-2023-34279	D-Link	D-Link DIR-2150 GetDeviceSettings Target Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-2150 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SOAP API interface, which listens on TCP port 80 by default. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20558.	2024-05-03	6.8	Medium
CVE-2023-34280	D-Link	D-Link DIR-2150 SetSysEmailSettings EmailTo Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-2150 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the SOAP API interface, which listens	2024-05-03	6.8	Medium

		on TCP port 80 by default. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20559.			
CVE-2023-34281	D-Link	D-Link DIR-2150 GetFirmwareStatus Target Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-2150 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the SOAP API interface, which listens on TCP port 80 by default. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20561.	2024-05-03	6.8	Medium
CVE-2023-41222	D-Link	D-Link DIR-3040 prog.cgi SetWan2Settings Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-3040 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-size stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21622.	2024-05-03	6.8	Medium
CVE-2023-41184	TP-Link	TP-Link Tapo C210 ActiveCells Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link Tapo C210 IP cameras. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of the ActiveCells parameter of the CreateRules and ModifyRules APIs. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20589.	2024-05-03	6.8	Medium
CVE-2023-41216	D-Link	D-Link DIR-3040 prog.cgi SetDynamicDNSSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-3040 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21616.	2024-05-03	6.8	Medium
CVE-2023-41218	D-Link	D-Link DIR-3040 prog.cgi SetWan3Settings Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-3040 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-size stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21618.	2024-05-03	6.8	Medium
CVE-2023-41219	D-Link	D-Link DIR-3040 prog.cgi SetWanSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-3040 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-size stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21619.	2024-05-03	6.8	Medium
CVE-2023-41220	D-Link	D-Link DIR-3040 prog.cgi SetSysEmailSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability	2024-05-03	6.8	Medium

		allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-3040 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-size stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21620.			
CVE-2023-41221	D-Link	D-Link DIR-3040 prog.cgi SetWLanRadioSecurity Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-3040 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-size stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21621.	2024-05-03	6.8	Medium
CVE-2023-41223	D-Link	D-Link DIR-3040 prog.cgi SetQuickVPNSettings PSK Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-3040 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-size stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21623.	2024-05-03	6.8	Medium
CVE-2023-41224	D-Link	D-Link DIR-3040 prog.cgi SetDeviceSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-3040 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-size stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21650.	2024-05-03	6.8	Medium
CVE-2023-41225	D-Link	D-Link DIR-3040 prog.cgi SetIPv6PppoeSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-3040 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-size stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21651.	2024-05-03	6.8	Medium
CVE-2023-41226	D-Link	D-Link DIR-3040 prog.cgi SetMyDLinkRegistration Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-3040 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-size stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21652.	2024-05-03	6.8	Medium
CVE-2023-41227	D-Link	D-Link DIR-3040 prog.cgi SetTriggerPPPoEValidate Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-3040 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-size	2024-05-03	6.8	Medium

		stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21653.			
CVE-2023-41228	D-Link	D-Link DIR-3040 prog.cgi SetUsersSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-3040 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-size stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21654.	2024-05-03	6.8	Medium
CVE-2023-44415	D-Link	D-Link Multiple Routers cli Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1260 and DIR-2150 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the CLI service, which listens on TCP port 23. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-19946.	2024-05-03	6.8	Medium
CVE-2023-44416	D-Link	D-Link DAP-2622 Telnet CLI Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2622. Authentication is required to exploit this vulnerability. The specific flaw exists within the CLI service, which listens on TCP port 23. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20051.	2024-05-03	6.8	Medium
CVE-2023-44448	TP-Link	TP-Link Archer A54 libcmm.so dm_fillObjByStr Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link Archer A54 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the file libcmm.so. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-22262.	2024-05-03	6.8	Medium
CVE-2023-50225	TP-Link	TP-Link TL-WR902AC dm_fillObjByStr Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link TL-WR902AC routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the libcmm.so module. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21819.	2024-05-03	6.8	Medium
CVE-2023-51613	D-Link	D-Link DIR-X3260 prog.cgi SetDynamicDNSSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21590.	2024-05-03	6.8	Medium
CVE-2023-51614	D-Link	D-Link DIR-X3260 prog.cgi SetQuickVPNSettings Password Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper	2024-05-03	6.8	Medium

		validation of a user-supplied string before copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21591.			
CVE-2023-51615	D-Link	D-Link DIR-X3260 prog.cgi SetQuickVPNSettings PSK Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21592.	2024-05-03	6.8	Medium
CVE-2023-51616	D-Link	D-Link DIR-X3260 prog.cgi SetSysEmailSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21593.	2024-05-03	6.8	Medium
CVE-2023-51617	D-Link	D-Link DIR-X3260 prog.cgi SetWanSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21594.	2024-05-03	6.8	Medium
CVE-2023-51618	D-Link	D-Link DIR-X3260 prog.cgi SetWLanRadioSecurity Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21595.	2024-05-03	6.8	Medium
CVE-2023-51619	D-Link	D-Link DIR-X3260 prog.cgi SetMyDLinkRegistration Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-size stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21667.	2024-05-03	6.8	Medium
CVE-2023-51620	D-Link	D-Link DIR-X3260 prog.cgi SetIPv6PppoeSettings Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-size stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21669.	2024-05-03	6.8	Medium

CVE-2023-51621	D-Link	D-Link DIR-X3260 prog.cgi SetDeviceSettings Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-size stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21670.	2024-05-03	6.8	Medium
CVE-2023-51622	D-Link	D-Link DIR-X3260 prog.cgi SetTriggerPPPoEValidate Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-size stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21672.	2024-05-03	6.8	Medium
CVE-2023-51623	D-Link	D-Link DIR-X3260 prog.cgi SetAPClientSettings Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-X3260 routers. Authentication is required to exploit this vulnerability. The specific flaw exists within the prog.cgi binary, which handles HNAP requests made to the lighttpd webserver listening on TCP ports 80 and 443. The issue results from the lack of proper validation of a user-supplied string before copying it to a fixed-size stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-21673.	2024-05-03	6.8	Medium
CVE-2023-27357	NETGEAR	NETGEAR RAX30 GetInfo Missing Authentication Information Disclosure Vulnerability. This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of NETGEAR RAX30 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of SOAP requests. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to disclose sensitive information, leading to further compromise. Was ZDI-CAN-19608.	2024-05-03	6.5	Medium
CVE-2023-32148	D-Link	D-Link DIR-2640 HNAP PrivateLogin Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-2640 routers. Authentication is not required to exploit this vulnerability.The specific flaw exists within the web management interface, which listens on TCP port 80 by default. A crafted XML element in the login request can cause authentication to succeed without providing proper credentials. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-19545.	2024-05-03	6.5	Medium
CVE-2023-32152	D-Link	D-Link DIR-2640 HNAP LoginPassword Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-2640 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the web management interface, which listens on TCP port 80 by default. A specially crafted login request can cause authentication to succeed without providing proper credentials. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-19549.	2024-05-03	6.5	Medium
CVE-2023-32167	D-Link	D-Link D-View uploadMib Directory Traversal Arbitrary File Creation or Deletion Vulnerability. This vulnerability allows remote attackers to create and delete arbitrary files on affected installations of D-Link D-View. Authentication is required to exploit this vulnerability. The specific flaw exists within the uploadMib function. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to create or delete files in the context of SYSTEM. Was ZDI-CAN-19529.	2024-05-03	6.5	Medium

CVE-2023-40512	LG	LG Simple Editor PlayerController getImageByFilename Directory Traversal Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of LG Simple Editor. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the getImageByFilename method in the PlayerController class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-20014.	2024-05-03	6.5	Medium
CVE-2023-40513	LG	LG Simple Editor UserManageController getImageByFilename Directory Traversal Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of LG Simple Editor. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the getImageByFilename method in the UserManageController class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-20015.	2024-05-03	6.5	Medium
CVE-2023-40514	LG	LG Simple Editor FileManagerController getImageByFilename Directory Traversal Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of LG Simple Editor. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the getImageByFilename method in the FileManagerController class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-20016.	2024-05-03	6.5	Medium
CVE-2023-41186	D-Link	D-Link DAP-1325 CGI Missing Authentication Information Disclosure Vulnerability. This vulnerability allows network-adjacent attackers to access various functionality on affected installations of D-Link DAP-1325 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the CGI interface. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-18804.	2024-05-03	6.5	Medium
CVE-2023-44447	TP-Link	TP-Link TL-WR902AC loginFs Improper Authentication Information Disclosure Vulnerability. This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of TP-Link TL-WR902AC routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the httpd service, which listens on TCP port 80 by default. The issue results from improper authentication. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-21529.	2024-05-03	6.5	Medium
CVE-2023-50224	TP-Link	TP-Link TL-WR841N dropbearpwd Improper Authentication Information Disclosure Vulnerability. This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of TP-Link TL-WR841N routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the httpd service, which listens on TCP port 80 by default. The issue results from improper authentication. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-19899.	2024-05-03	6.5	Medium
CVE-2023-34284	NETGEAR	NETGEAR RAX30 Use of Hard-coded Credentials Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR RAX30 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the system configuration. The system contains a hardcoded user account which can be used to access the CLI service as a low-privileged user. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-19660.	2024-05-03	6.3	Medium

CVE-2023-51629	D-Link	D-Link DCS-8300LHV2 ONVIF Hardcoded PIN Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DCS-8300LHV2 IP cameras. Authentication is not required to exploit this vulnerability. The specific flaw exists within the configuration of the ONVIF API. The issue results from the use of a hardcoded PIN. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-21492.	2024-05-03	6.3	Medium
CVE-2023-38724	IBM	IBM Cognos Controller 10.4.1, 10.4.2, and 11.0.0 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 262183.	2024-05-03	6.3	Medium
CVE-2023-40695	IBM	IBM Cognos Controller 10.4.1, 10.4.2, and 11.0.0 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 264938.	2024-05-03	6.3	Medium
CVE-2021-20451	IBM	IBM Cognos Controller 10.4.1, 10.4.2, and 11.0.0 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 196643.	2024-05-03	6	Medium
CVE-2023-44413	D-Link	D-Link D-View shutdown_coreserver Missing Authentication Denial-of-Service Vulnerability. This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of D-Link D-View. Authentication is not required to exploit this vulnerability. The specific flaw exists within the shutdown_coreserver action. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-19572.	2024-05-03	5.9	Medium
CVE-2020-4874	IBM	IBM Cognos Controller 10.4.1, 10.4.2, and 11.0.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 190837.	2024-05-03	5.9	Medium
CVE-2023-40696	IBM	IBM Cognos Controller 10.4.1, 10.4.2, and 11.0.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 264939.	2024-05-03	5.9	Medium
CVE-2023-27370	NETGEAR	NETGEAR RAX30 Device Configuration Cleartext Storage Information Disclosure Vulnerability. This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of NETGEAR RAX30 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of device configuration. The issue results from the storage of configuration secrets in plaintext. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-19841.	2024-05-03	5.7	Medium
CVE-2023-41181	LG	LG SuperSign Media Editor getSubFolderList Directory Traversal Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of LG SuperSign Media Editor. Authentication is not required to exploit this vulnerability. The specific flaw exists within the getSubFolderList method. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-20330.	2024-05-03	5.3	Medium
CVE-2021-20556	IBM	IBM Cognos Controller 10.4.1, 10.4.2, and 11.0.0 could allow a remote user to enumerate usernames due to differentiating error messages on existing usernames. IBM X-Force ID: 199181.	2024-05-03	5.3	Medium
CVE-2023-28952	IBM	IBM Cognos Controller 10.4.1, 10.4.2, and 11.0.0 is vulnerable to injection attacks in application logging by not sanitizing user provided data. IBM X-Force ID: 251463.	2024-05-03	5.3	Medium
CVE-2022-22364	IBM	IBM Cognos Controller 10.4.1, 10.4.2, and 11.0.0 is vulnerable to external service interaction attack, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability to induce the application to perform server-side DNS lookups or HTTP requests to arbitrary domain names. By submitting suitable payloads, an attacker can cause the application server to attack other systems that it can interact with. IBM X-Force ID: 220903.	2024-05-03	5.3	Medium

CVE-2023-34283	NETGEAR	NETGEAR RAX30 USB Share Link Following Information Disclosure Vulnerability. This vulnerability allows physically present attackers to disclose sensitive information on affected installations of NETGEAR RAX30 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of symbolic links on removable USB media. By creating a symbolic link, an attacker can abuse the router's web server to access arbitrary local files. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-19498.	2024-05-03	4.6	Medium
CVE-2023-32137	D-Link	D-Link DAP-1360 webproc WEB_DisplayPage Directory Traversal Information Disclosure Vulnerability. This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of D-Link DAP-1360 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of requests to the /cgi-bin/webproc endpoint. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-18415.	2024-05-03	4.3	Medium
CVE-2023-50212	D-Link	D-Link G416 httpd Improper Handling of Exceptional Conditions Information Disclosure Vulnerability. This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of D-Link G416 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HTTP service listening on TCP port 80. The issue results from the lack of proper handling of error conditions. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of root. Was ZDI-CAN-21664.	2024-05-03	4.3	Medium
CVE-2021-20450	IBM	IBM Cognos Controller 10.4.1, 10.4.2, and 11.0.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 196640.	2024-05-03	4.3	Medium
CVE-2023-27283	IBM	IBM Aspera Orchestrator 4.0.1 could allow a remote attacker to enumerate usernames due to observable response discrepancies. IBM X-Force ID: 248545.	2024-05-04	5.3	Medium

Where NCA provides the vulnerability information as published by NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. وإذ تبقى مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة.