الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

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

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 29 مارس إلى 4 أبريل. 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

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

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 29th of March to 4th of April. 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 |
|---|---|---|---|---|
| CVE-2026-32213 | microsoft - azure_ai_foundry | Improper authorization in Azure AI Foundry allows an unauthorized attacker to elevate privileges over a network. | 2026-04-03 | 10 |
| CVE-2026-33105 | microsoft - azure_kubernetes_service | Improper authorization in Microsoft Azure Kubernetes Service allows an unauthorized attacker to elevate privileges over a network. | 2026-04-03 | 10 |
| CVE-2026-33107 | microsoft - azure_databricks | Server-side request forgery (ssrf) in Azure Databricks allows an unauthorized attacker to elevate privileges over a network. | 2026-04-03 | 10 |
| CVE-2026-32186 | microsoft - Microsoft Bing | Server-side request forgery (ssrf) in Microsoft Bing allows an unauthorized attacker to elevate privileges over a network. | 2026-04-03 | 10 |
| CVE-2026-5121 | red hat - multiple products | A flaw was found in libarchive. On 32-bit systems, an integer overflow vulnerability exists in the zisofs block pointer allocation logic. A remote attacker can exploit this by providing a specially crafted ISO9660 image, which can lead to a heap buffer overflow. This could potentially allow for arbitrary code execution on the affected system. | 2026-03-30 | 9.8 |
| CVE-2026-20093 | cisco - multiple products | A vulnerability in the change password functionality of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to bypass authentication and gain access to the system as Admin._x000D_ _x000D_ This vulnerability is due to incorrect handling of password change requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to bypass authentication, alter the passwords of any user on the system, including an Admin user, and gain access to the system as that user. | 2026-04-01 | 9.8 |
| CVE-2026-20160 | cisco - Cisco Smart Software Manager On-Prem | A vulnerability in Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected SSM On-Prem host._x000D_ _x000D_ This vulnerability is due to the unintentional exposure of an internal service. An attacker could exploit this vulnerability by sending a crafted request to the API of the exposed service. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. | 2026-04-01 | 9.8 |
| CVE-2026-35616 | fortinet - multiple products | A improper access control vulnerability in Fortinet FortiClientEMS 7.4.5 through 7.4.6 may allow an unauthenticated attacker to execute unauthorized code or commands via crafted requests. | 2026-04-04 | 9.8 |
| CVE-2026-5288 | google - chrome | Use after free in WebView in Google Chrome on Android prior to 146.0.7680.178 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High) | 2026-04-01 | 9.6 |
| CVE-2026-5289 | google - chrome | Use after free in Navigation in Google Chrome prior to 146.0.7680.178 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High) | 2026-04-01 | 9.6 |
| CVE-2026-5290 | google - chrome | Use after free in Compositing in Google Chrome prior to 146.0.7680.178 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High) | 2026-04-01 | 9.6 |
| CVE-2026-26135 | microsoft - azure_custom_locations_resource_provider | Server-side request forgery (ssrf) in Azure Custom Locations Resource Provider (RP) allows an authorized attacker to elevate privileges over a network. | 2026-04-03 | 9.6 |
| CVE-2026-32211 | microsoft - azure_web_apps | Missing authentication for critical function in Azure MCP Server allows an unauthorized attacker to disclose information over a network. | 2026-04-03 | 9.1 |

| | | | | |
|---|---|---|---|---|
| CVE-2026-5272 | google - chrome | Heap buffer overflow in GPU in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High) | 2026-04-01 | 8.8 |
| CVE-2026-5274 | google - chrome | Integer overflow in Codecs in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High) | 2026-04-01 | 8.8 |
| CVE-2026-5275 | google - chrome | Heap buffer overflow in ANGLE in Google Chrome on Mac prior to 146.0.7680.178 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High) | 2026-04-01 | 8.8 |
| CVE-2026-5278 | google - chrome | Use after free in Web MIDI in Google Chrome on Android prior to 146.0.7680.178 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High) | 2026-04-01 | 8.8 |
| CVE-2026-5279 | google - chrome | Object corruption in V8 in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High) | 2026-04-01 | 8.8 |
| CVE-2026-5280 | google - chrome | Use after free in WebCodecs in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High) | 2026-04-01 | 8.8 |
| CVE-2026-5281 | google - chrome | Use after free in Dawn in Google Chrome prior to 146.0.7680.178 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page. (Chromium security severity: High) | 2026-04-01 | 8.8 |
| CVE-2026-5285 | google - chrome | Use after free in WebGL in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High) | 2026-04-01 | 8.8 |
| CVE-2026-5286 | google - chrome | Use after free in Dawn in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High) | 2026-04-01 | 8.8 |
| CVE-2026-5287 | google - chrome | Use after free in PDF in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: High) | 2026-04-01 | 8.8 |
| CVE-2026-5292 | google - chrome | Out of bounds read in WebCodecs in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium) | 2026-04-01 | 8.8 |
| CVE-2026-20094 | cisco - multiple products | A vulnerability in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with read-only privileges to perform command injection attacks on an affected system and execute arbitrary commands as the root user._x000D_<br>_x000D_<br>This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted commands to the web-based management interface of the affected software. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system as the root user. | 2026-04-01 | 8.8 |
| CVE-2025-43202 | apple - multiple products | This issue was addressed with improved memory handling. This issue is fixed in iOS 18.6 and iPadOS 18.6, macOS Sequoia 15.6. Processing a file may lead to memory corruption. | 2026-04-02 | 8.8 |
| CVE-2025-43219 | apple - macos | The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.6. Processing a maliciously crafted image may corrupt process memory. | 2026-04-02 | 8.8 |
| CVE-2025-43264 | apple - macos | The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.6. Processing a maliciously crafted image may corrupt process memory. | 2026-04-02 | 8.8 |
| CVE-2026-34121 | tp-link - tapo_c520ws_firmware | An authentication bypass vulnerability within the HTTP handling of the DS configuration service in TP-Link Tapo C520WS v2.6 was identified, due to inconsistent parsing and authorization logic in JSON requests during authentication check. An unauthenticated attacker can append an authentication-exempt action to a request containing privileged DS do actions, bypassing authorization checks.<br><br>Successful exploitation allows unauthenticated execution of restricted configuration actions, which may result in unauthorized modification of device state. | 2026-04-02 | 8.7 |
| CVE-2025-43257 | apple - macos | This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sequoia 15.6. An app may be able to break out of its sandbox. | 2026-04-02 | 8.7 |
| CVE-2026-2123 | microfocus - operations_agent | A security audit identified a privilege escalation<br>vulnerability in Operations Agent(<=OA 12.29) on Windows. Under specific conditions<br>Operations Agent may run executables from specific writeable locations.Thanks to Manuel Rickli &<br>Philippe Leiser of<br>Oneconsult AG for reporting this vulnerability | 2026-03-31 | 8.6 |
| CVE-2026-3987 | watchguard - Fireware OS | A path traversal vulnerability in the Fireware OS Web UI on WatchGuard Firebox systems may allow a privileged authenticated remote attacker to execute arbitrary code in the context of an elevated system process.This issue affects Fireware OS 12.6.1 up to and including 12.11.8 and 2025.1 up to and including 2026.1.2. | 2026-04-01 | 8.6 |
| CVE-2026-32173 | microsoft - azure_sre_agent | Improper authentication in Azure SRE Agent allows an unauthorized attacker to disclose information over a network. | 2026-04-03 | 8.6 |
| CVE-2026-4266 | watchguard - Fireware OS | An Insecure Deserialization vulnerability in WatchGuard Fireware OS allows an attacker that has obtained write access to the local filesystem through another vulnerability to execute arbitrary code in the context of the portald user.This issue affects Fireware OS: 12.1 through 12.11.8 and 2025.1 through 2026.1.2.<br><br>Note, this vulnerability does not affect Firebox platforms that do not support the Access Portal feature, including the T-15 and T-35. | 2026-03-30 | 8.4 |
| CVE-2024-44250 | apple - macos | A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.1. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges. | 2026-04-02 | 8.2 |
| CVE-2026-5282 | google - chrome | Out of bounds read in WebCodecs in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High) | 2026-04-01 | 8.1 |
| CVE-2026-4101 | ibm - multiple products | IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 under certain load conditions could allow an attacker to bypass authentication mechanisms and gain unauthorized access to the application. | 2026-04-01 | 8.1 |

| | | | | |
|---|---|---|---|---|
| CVE-2026-4636 | red hat - multiple products | A flaw was found in Keycloak. An authenticated user with the uma_protection role can bypass User-Managed Access (UMA) policy validation. This allows the attacker to include resource identifiers owned by other users in a policy creation request, even if the URL path specifies an attacker-owned resource. Consequently, the attacker gains unauthorized permissions to victim-owned resources, enabling them to obtain a Requesting Party Token (RPT) and access sensitive information or perform unauthorized actions. | 2026-04-02 | 8.1 |
| CVE-2026-20155 | cisco - Cisco Evolved Programmable Network Manager (EPNM) | A vulnerability in the web-based management interface of Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker with low privileges to access sensitive information that they are not authorized to access._x000D_<br>_x000D_<br>This vulnerability is due to improper authorization checks on a REST API endpoint of an affected device. An attacker could exploit this vulnerability by querying the affected endpoint. A successful exploit could allow the attacker to view session information of active Cisco EPNM users, including users with administrative privileges, which could result in the affected device being compromised. | 2026-04-01 | 8 |
| CVE-2026-34054 | microsoft - vcpkg | vcpkg is a free and open-source C/C++ package manager. Prior to version 3.6.1#3, vcpkg's Windows builds of OpenSSL set openssldir to a path on the build machine, making that path be attackable later on customer machines. This issue has been patched in version 3.6.1#3. | 2026-03-31 | 7.8 |
| CVE-2026-23406 | linux - multiple products | In the Linux kernel, the following vulnerability has been resolved:<br><br>apparmor: fix side-effect bug in match_char() macro usage<br><br>The match_char() macro evaluates its character parameter multiple<br>times when traversing differential encoding chains. When invoked<br>with *str++, the string pointer advances on each iteration of the<br>inner do-while loop, causing the DFA to check different characters<br>at each iteration and therefore skip input characters.<br>This results in out-of-bounds reads when the pointer advances past<br>the input buffer boundary.<br><br>[ 94.984676] ==========<br>[ 94.985301] BUG: KASAN: slab-out-of-bounds in aa_dfa_match+0x5ae/0x760<br>[ 94.985655] Read of size 1 at addr ffff888100342000 by task file/976<br><br>[ 94.986319] CPU: 7 UID: 1000 PID: 976 Comm: file Not tainted 6.19.0-rc7-next-20260127 #1 PREEMPT(lazy)<br>[ 94.986322] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014<br>[ 94.986329] Call Trace:<br>[ 94.986341] <TASK><br>[ 94.986347] dump_stack_lvl+0x5e/0x80<br>[ 94.986374] print_report+0xc8/0x270<br>[ 94.986384] ? aa_dfa_match+0x5ae/0x760<br>[ 94.986388] kasan_report+0x118/0x150<br>[ 94.986401] ? aa_dfa_match+0x5ae/0x760<br>[ 94.986405] aa_dfa_match+0x5ae/0x760<br>[ 94.986408] __aa_path_perm+0x131/0x400<br>[ 94.986418] aa_path_perm+0x219/0x2f0<br>[ 94.986424] apparmor_file_open+0x345/0x570<br>[ 94.986431] security_file_open+0x5c/0x140<br>[ 94.986442] do_dentry_open+0x2f6/0x1120<br>[ 94.986450] vfs_open+0x38/0x2b0<br>[ 94.986453] ? may_open+0x1e2/0x2b0<br>[ 94.986466] path_openat+0x231b/0x2b30<br>[ 94.986469] ? __x64_sys_openat+0xf8/0x130<br>[ 94.986477] do_file_open+0x19d/0x360<br>[ 94.986487] do_sys_openat2+0x98/0x100<br>[ 94.986491] __x64_sys_openat+0xf8/0x130<br>[ 94.986499] do_syscall_64+0x8e/0x660<br>[ 94.986515] ? count_memcg_events+0x15f/0x3c0<br>[ 94.986526] ? srso_alias_return_thunk+0x5/0xfbef5<br>[ 94.986540] ? handle_mm_fault+0x1639/0x1ef0<br>[ 94.986551] ? vma_start_read+0xf0/0x320<br>[ 94.986558] ? srso_alias_return_thunk+0x5/0xfbef5<br>[ 94.986561] ? srso_alias_return_thunk+0x5/0xfbef5<br>[ 94.986563] ? fpregs_assert_state_consistent+0x50/0xe0<br>[ 94.986572] ? srso_alias_return_thunk+0x5/0xfbef5<br>[ 94.986574] ? arch_exit_to_user_mode_prepare+0x9/0xb0<br>[ 94.986587] ? srso_alias_return_thunk+0x5/0xfbef5<br>[ 94.986588] ? irqentry_exit+0x3c/0x590<br>[ 94.986595] entry_SYSCALL_64_after_hwframe+0x76/0x7e<br>[ 94.986597] RIP: 0033:0x7fda4a79c3ea<br><br>Fix by extracting the character value before invoking match_char,<br>ensuring single evaluation per outer loop. | 2026-04-01 | 7.8 |
| CVE-2026-23407 | linux - multiple products | In the Linux kernel, the following vulnerability has been resolved:<br><br>apparmor: fix missing bounds check on DEFAULT table in verify_dfa()<br><br>The verify_dfa() function only checks DEFAULT_TABLE bounds when the state | 2026-04-01 | 7.8 |

| | | | | |
|---|---|---|---|---|
| | | is not differentially encoded.<br><br>When the verification loop traverses the differential encoding chain,<br>it reads k = DEFAULT_TABLE[j] and uses k as an array index without<br>validation. A malformed DFA with DEFAULT_TABLE[j] >= state_count,<br>therefore, causes both out-of-bounds reads and writes.<br><br>[ 57.179855] ==========<br>[ 57.180549] BUG: KASAN: slab-out-of-bounds in verify_dfa+0x59a/0x660<br>[ 57.180904] Read of size 4 at addr ffff888100eadec4 by task su/993<br><br>[ 57.181554] CPU: 1 UID: 0 PID: 993 Comm: su Not tainted 6.19.0-rc7-next-20260127 #1<br>PREEMPT(lazy)<br>[ 57.181558] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2<br>04/01/2014<br>[ 57.181563] Call Trace:<br>[ 57.181572] <TASK><br>[ 57.181577] dump_stack_lvl+0x5e/0x80<br>[ 57.181596] print_report+0xc8/0x270<br>[ 57.181605] ? verify_dfa+0x59a/0x660<br>[ 57.181608] kasan_report+0x118/0x150<br>[ 57.181620] ? verify_dfa+0x59a/0x660<br>[ 57.181623] verify_dfa+0x59a/0x660<br>[ 57.181627] aa_dfa_unpack+0x1610/0x1740<br>[ 57.181629] ? __kmalloc_cache_noprof+0x1d0/0x470<br>[ 57.181640] unpack_pdb+0x86d/0x46b0<br>[ 57.181647] ? srso_alias_return_thunk+0x5/0xfbef5<br>[ 57.181653] ? srso_alias_return_thunk+0x5/0xfbef5<br>[ 57.181656] ? aa_unpack_nameX+0x1a8/0x300<br>[ 57.181659] aa_unpack+0x20b0/0x4c30<br>[ 57.181662] ? srso_alias_return_thunk+0x5/0xfbef5<br>[ 57.181664] ? stack_depot_save_flags+0x33/0x700<br>[ 57.181681] ? kasan_save_track+0x4f/0x80<br>[ 57.181683] ? kasan_save_track+0x3e/0x80<br>[ 57.181686] ? __kasan_kmalloc+0x93/0xb0<br>[ 57.181688] ? __kvmalloc_node_noprof+0x44a/0x780<br>[ 57.181693] ? aa_simple_write_to_buffer+0x54/0x130<br>[ 57.181697] ? policy_update+0x154/0x330<br>[ 57.181704] aa_replace_profiles+0x15a/0x1dd0<br>[ 57.181707] ? srso_alias_return_thunk+0x5/0xfbef5<br>[ 57.181710] ? __kvmalloc_node_noprof+0x44a/0x780<br>[ 57.181712] ? aa_loaddata_alloc+0x77/0x140<br>[ 57.181715] ? srso_alias_return_thunk+0x5/0xfbef5<br>[ 57.181717] ? _copy_from_user+0x2a/0x70<br>[ 57.181730] policy_update+0x17a/0x330<br>[ 57.181733] profile_replace+0x153/0x1a0<br>[ 57.181735] ? rw_verify_area+0x93/0x2d0<br>[ 57.181740] vfs_write+0x235/0xab0<br>[ 57.181745] ksys_write+0xb0/0x170<br>[ 57.181748] do_syscall_64+0x8e/0x660<br>[ 57.181762] entry_SYSCALL_64_after_hwframe+0x76/0x7e<br>[ 57.181765] RIP: 0033:0x7f6192792eb2<br><br>Remove the MATCH_FLAG_DIFF_ENCODE condition to validate all DEFAULT_TABLE<br>entries unconditionally. | | |
| CVE-2026-23408 | linux - multiple products | In the Linux kernel, the following vulnerability has been resolved:<br><br>apparmor: Fix double free of ns_name in aa_replace_profiles()<br><br>if ns_name is NULL after<br>1071 error = aa_unpack(udata, &lh, &ns_name);<br><br>and if ent->ns_name contains an ns_name in<br>1089 } else if (ent->ns_name) {<br><br>then ns_name is assigned the ent->ns_name<br>1095 ns_name = ent->ns_name;<br><br>however ent->ns_name is freed at<br>1262 aa_load_ent_free(ent);<br><br>and then again when freeing ns_name at<br>1270 kfree(ns_name);<br><br>Fix this by NULLing out ent->ns_name after it is transferred to ns_name<br><br>") | 2026-04-01 | 7.8 |
| CVE-2026-23410 | linux - multiple products | In the Linux kernel, the following vulnerability has been resolved:<br><br>apparmor: fix race on rawdata dereference | 2026-04-01 | 7.8 |

| | | | | |
|---|---|---|---|---|
| | | There is a race condition that leads to a use-after-free situation: because the rawdata inodes are not refcounted, an attacker can start open()ing one of the rawdata files, and at the same time remove the last reference to this rawdata (by removing the corresponding profile, for example), which frees its struct aa_loaddata; as a result, when seq_rawdata_open() is reached, i_private is a dangling pointer and freed memory is accessed.<br><br>The rawdata inodes weren't refcounted to avoid a circular refcount and were supposed to be held by the profile rawdata reference. However during profile removal there is a window where the vfs and profile destruction race, resulting in the use after free.<br><br>Fix this by moving to a double refcount scheme. Where the profile refcount on rawdata is used to break the circular dependency. Allowing for freeing of the rawdata once all inode references to the rawdata are put. | | |
| CVE-2026-23411 | linux - multiple products | In the Linux kernel, the following vulnerability has been resolved:<br><br>apparmor: fix race between freeing data and fs accessing it<br><br>AppArmor was putting the reference to i_private data on its end after removing the original entry from the file system. However the inode can aand does live beyond that point and it is possible that some of the fs call back functions will be invoked after the reference has been put, which results in a race between freeing the data and accessing it through the fs.<br><br>While the rawdata/loaddata is the most likely candidate to fail the race, as it has the fewest references. If properly crafted it might be possible to trigger a race for the other types stored in i_private.<br><br>Fix this by moving the put of i_private referenced data to the correct place which is during inode eviction. | 2026-04-01 | 7.8 |
| CVE-2025-13855 | ibm - storage_protect_server | IBM Storage Protect Server 8.2.0 IBM Storage Protect Plus Server 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. | 2026-04-01 | 7.6 |
| CVE-2026-4046 | gnu - glibc | The iconv() function in the GNU C Library versions 2.43 and earlier may crash due to an assertion failure when converting inputs from the IBM1390 or IBM1399 character sets, which may be used to remotely crash an application.<br><br>This vulnerability can be trivially mitigated by removing the IBM1390 and IBM1399 character sets from systems that do not need them. | 2026-03-30 | 7.5 |
| CVE-2026-5201 | red hat - multiple products | A flaw was found in the gdk-pixbuf library. This heap-based buffer overflow vulnerability occurs in the JPEG image loader due to improper validation of color component counts when processing a specially crafted JPEG image. A remote attacker can exploit this flaw without user interaction, for example, via thumbnail generation. Successful exploitation leads to application crashes and denial of service (DoS) conditions. | 2026-03-31 | 7.5 |
| CVE-2026-5277 | google - chrome | Integer overflow in ANGLE in Google Chrome on Windows prior to 146.0.7680.178 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High) | 2026-04-01 | 7.5 |
| CVE-2026-5284 | google - chrome | Use after free in Dawn in Google Chrome prior to 146.0.7680.178 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page. (Chromium security severity: High) | 2026-04-01 | 7.5 |
| CVE-2026-4634 | red hat - multiple products | A flaw was found in Keycloak. An unauthenticated attacker can exploit this vulnerability by sending a specially crafted POST request with an excessively long scope parameter to the OpenID Connect (OIDC) token endpoint. This leads to high resource consumption and prolonged processing times, ultimately resulting in a Denial of Service (DoS) for the Keycloak server. | 2026-04-02 | 7.5 |
| CVE-2025-58136 | apache - multiple products | A bug in POST request handling causes a crash under a certain condition.<br><br>This issue affects Apache Traffic Server: from 10.0.0 through 10.1.1, from 9.0.0 through 9.2.12.<br><br>Users are recommended to upgrade to version 10.1.2 or 9.2.13, which fix the issue.<br><br>A workaround for older versions is to set proxy.config.http.request_buffer_enabled to 0 (the default value is 0). | 2026-04-02 | 7.5 |
| CVE-2025-65114 | apache - multiple products | Apache Traffic Server allows request smuggling if chunked messages are malformed.<br><br>This issue affects Apache Traffic Server: from 9.0.0 through 9.2.12, from 10.0.0 through 10.1.1.<br><br>Users are recommended to upgrade to version 9.2.13 or 10.1.2, which fix the issue. | 2026-04-02 | 7.5 |
| CVE-2026-35385 | openbsd - OpenSSH | In OpenSSH before 10.3, a file downloaded by scp may be installed setuid or setgid, an outcome contrary to some users' expectations, if the download is performed as root with -O (legacy scp protocol) and without -p (preserve mode). | 2026-04-02 | 7.5 |
| CVE-2024-40849 | apple - macos | A race condition was addressed with additional validation. This issue is fixed in macOS Sequoia 15.1. An app may be able to break out of its sandbox. | 2026-04-02 | 7.5 |

| | | | | |
|---|---|---|---|---|
| CVE-2024-44219 | apple - macos | A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.1. A malicious application with root privileges may be able to access private information. | 2026-04-02 | 7.5 |
| CVE-2024-44286 | apple - macos | This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15.1. An attacker with physical access can input keyboard events to apps running on a locked device. | 2026-04-02 | 7.5 |
| CVE-2024-44303 | apple - macos | The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.1. A malicious application may be able to modify protected parts of the file system. | 2026-04-02 | 7.5 |
| CVE-2026-28815 | apple - macOS | A remote attacker can supply a short X-Wing HPKE encapsulated key and trigger an out-of-bounds read in the C decapsulation path, potentially causing a crash or memory disclosure depending on runtime protections. This issue is fixed in swift-crypto version 4.3.1. | 2026-04-03 | 7.5 |
| CVE-2026-4282 | red hat - multiple products | A flaw was found in Keycloak. The SingleUseObjectProvider, a global key-value store, lacks proper type and namespace isolation. This vulnerability allows an unauthenticated attacker to forge authorization codes. Successful exploitation can lead to the creation of admin-capable access tokens, resulting in privilege escalation. | 2026-04-02 | 7.4 |
| CVE-2026-5349 | trendnet - tew-657brm_firmware | A vulnerability was identified in Trendnet TEW-657BRM 1.00.1. The affected element is the function add_apcdb of the file /setup.cgi. The manipulation of the argument mac_pc_dba leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit is publicly available and might be used. The vendor confirms, that "[t]he product in question (...) has been discontinued and end of life since June 23, 2011, that is more than 14 years ago. We no longer provide support for this product, so we are not able to confirm the vulnerabilities. We will make an announcement on our website's product support page and notify customers who registered their products with us." This vulnerability only affects products that are no longer supported by the maintainer. | 2026-04-02 | 7.4 |
| CVE-2026-5350 | trendnet - tew-657brm_firmware | A security flaw has been discovered in Trendnet TEW-657BRM 1.00.1. The impacted element is the function update_pcdb of the file /setup.cgi. The manipulation of the argument mac_pc_dba results in stack-based buffer overflow. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. The vendor confirms, that "[t]he product in question (...) has been discontinued and end of life since June 23, 2011, that is more than 14 years ago. We no longer provide support for this product, so we are not able to confirm the vulnerabilities. We will make an announcement on our website's product support page and notify customers who registered their products with us." This vulnerability only affects products that are no longer supported by the maintainer. | 2026-04-02 | 7.4 |
| CVE-2026-22767 | dell - appsync | Dell AppSync, version(s) 4.6.0, contain(s) an UNIX Symbolic Link (Symlink) Following vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information tampering. | 2026-04-01 | 7.3 |
| CVE-2026-22768 | dell - appsync | Dell AppSync, version(s) 4.6.0, contain(s) an Incorrect Permission Assignment for Critical Resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges. | 2026-04-01 | 7.3 |
| CVE-2026-20151 | cisco - Cisco Smart Software Manager On-Prem | A vulnerability in the web interface of Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an authenticated, remote attacker to elevate privileges on an affected system._x000D_ _x000D_ This vulnerability is due to the improper transmission of sensitive user information. An attacker could exploit this vulnerability by sending a crafted message to an affected Cisco SSM On-Prem host and retrieving session credentials from subsequent status messages. A successful exploit could allow the attacker to elevate privileges on the affected system from low to administrative._x000D_ To exploit this vulnerability, the attacker must have valid credentials for a user account with at least the role of System User._x000D_ Note: This vulnerability exposes information only about users who logged in to the Cisco SSM On-Prem host using the web interface and who are currently logged in. SSH sessions are not affected. | 2026-04-01 | 7.3 |
| CVE-2026-1345 | ibm - multiple products | IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 could allow an unauthenticated user to execute arbitrary commands as lower user privileges on the system due to improper validation of user supplied input. | 2026-04-01 | 7.3 |
| CVE-2026-3872 | red hat - multiple products | A flaw was found in Keycloak. This issue allows an attacker, who controls another path on the same web server, to bypass the allowed path in redirect Uniform Resource Identifiers (URIs) that use a wildcard. A successful attack may lead to the theft of an access token, resulting in information disclosure. | 2026-04-02 | 7.3 |
| CVE-2026-28754 | zohocorp - multiple products | Zohocorp ManageEngine Exchange Reporter Plus versions before 5802 are vulnerable to Stored XSS in Distribution Lists report. | 2026-04-03 | 7.3 |
| CVE-2026-28756 | zohocorp - multiple products | Zohocorp ManageEngine Exchange Reporter Plus versions before 5802 are vulnerable to Stored XSS in Permissions based on Distribution Groups report. | 2026-04-03 | 7.3 |
| CVE-2026-28703 | zohocorp - multiple products | Zohocorp ManageEngine Exchange Reporter Plus versions before 5802 are vulnerable to Stored XSS in Mails Exchanged Between Users report. | 2026-04-03 | 7.3 |
| CVE-2026-3879 | zohocorp - multiple products | Zohocorp ManageEngine Exchange Reporter Plus versions before 5802 are vulnerable to Stored XSS in Equipment Mailbox Details report. | 2026-04-03 | 7.3 |
| CVE-2026-3880 | zohocorp - multiple products | Zohocorp ManageEngine Exchange Reporter Plus versions before 5802 are vulnerable to Stored XSS in Public Folder Client Permissions report. | 2026-04-03 | 7.3 |
| CVE-2026-4107 | zohocorp - multiple products | Zohocorp ManageEngine Exchange Reporter Plus versions before 5802 are vulnerable to Stored XSS in Folder Message Count and Size report. | 2026-04-03 | 7.3 |
| CVE-2026-4108 | zohocorp - multiple products | Zohocorp ManageEngine Exchange Reporter Plus versions before 5802 are vulnerable to Stored XSS in Non-Owner Mailbox Permission report. | 2026-04-03 | 7.3 |
| CVE-2026-27655 | zohocorp - multiple products | Zohocorp ManageEngine Exchange Reporter Plus versions before 5802 are vulnerable to Stored XSS in Permissions Based on Mailboxes report. | 2026-04-03 | 7.3 |
| CVE-2026-4315 | watchguard - Fireware OS | A Cross-Site Request Forgery (CSRF) vulnerability in the WatchGuard Fireware OS WebUI could allow a remote attacker to trigger a denial-of-service (DoS) condition in the Fireware Web UI by convincing an authenticated administrator into visiting a malicious web page.This issue affects Fireware OS: 11.8 through 11.12.4+541730, 12.0 through 12.11.8, and 2025.1 through 2026.1.2. | 2026-03-30 | 7.1 |
| CVE-2026-34118 | tp-link - tapo_c520ws_firmware | A heap-based buffer overflow vulnerability was identified in TP-Link Tapo C520WS v2.6 in the HTTP POST body parsing logic due to missing validation of remaining buffer capacity after dynamic allocation, due to insufficient boundary validation when handling externally supplied HTTP | 2026-04-02 | 7.1 |

| | | | | |
|---|---|---|---|---|
| | | input. An attacker<br>on the same network segment could trigger heap memory corruption conditions by<br>sending crafted payloads that cause write operations beyond allocated buffer<br>boundaries. Successful exploitation<br>causes a Denial-of-Service (DoS) condition, causing the device's process to<br>crash or become unresponsive. | | |
| CVE-2026-34119 | tp-link - tapo_c520ws_firmware | A heap-based buffer overflow vulnerability was identified in TP-Link Tapo C520WS v2.6 within the HTTP parsing<br>loop<br>when appending segmented request bodies without<br>continuous write-boundary verification, due to insufficient boundary validation when handling<br>externally supplied HTTP input. An attacker<br>on the same network segment could trigger heap memory corruption conditions by<br>sending crafted payloads that cause write operations beyond allocated buffer<br>boundaries. Successful exploitation<br>causes a Denial-of-Service (DoS) condition, causing the device's process to<br>crash or become unresponsive. | 2026-04-02 | 7.1 |
| CVE-2026-34120 | tp-link - tapo_c520ws_firmware | A heap-based buffer overflow vulnerability was identified in TP-Link Tapo C520WS v2.6 within the asynchronous parsing of local video stream content due to<br>insufficient alignment and validation of buffer boundaries when processing streaming inputs.An attacker<br>on the same network segment could trigger heap memory corruption conditions by<br>sending crafted payloads that cause write operations beyond allocated buffer<br>boundaries. Successful exploitation<br>causes a Denial-of-Service (DoS) condition, causing the device's process to<br>crash or become unresponsive. | 2026-04-02 | 7.1 |
| CVE-2026-34122 | tp-link - tapo_c520ws_firmware | A stack-based buffer overflow vulnerability was identified in TP-Link Tapo C520WS v2.6 within a configuration handling component due to insufficient input validation. An attacker can exploit this vulnerability by supplying an excessively long value for a vulnerable configuration parameter, resulting in a stack overflow.<br><br>Successful exploitation results in Denial-of-Service (DoS) condition, leading to a service crash or device reboot, impacting availability. | 2026-04-02 | 7.1 |
| CVE-2026-34124 | tp-link - tapo_c520ws_firmware | A denial-of-service vulnerability was identified in TP-Link Tapo C520WS v2.6 within the HTTP request path parsing logic. The implementation enforces length restrictions on the raw request path but does not account for path expansion performed during normalization. An attacker on the adjacent network may send a crafted HTTP request to cause buffer overflow and memory corruption, leading to system interruption or device reboot. | 2026-04-02 | 7.1 |
| CVE-2024-40858 | apple - macos | A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.1. An app may be able to access Contacts without user consent. | 2026-04-02 | 7.1 |
| CVE-2026-33990 | docker - model-runner | Docker Model Runner (DMR) is software used to manage, run, and deploy AI models using Docker. Prior to version 1.1.25, Docker Model Runner contains an SSRF vulnerability in its OCI registry token exchange flow. When pulling a model, Model Runner follows the realm URL from the registry's WWW-Authenticate header without validating the scheme, hostname, or IP range. A malicious OCI registry can set the realm to an internal URL (e.g., http://127.0.0.1:3000/), causing Model Runner running on the host to make arbitrary GET requests to internal services and reflect the full response body back to the caller. Additionally, the token exchange mechanism can relay data from internal services back to the attacker-controlled registry via the Authorization: Bearer header. This issue has been patched in version 1.1.25. For Docker Desktop users, enabling Enhanced Container Isolation (ECI) blocks container access to Model Runner, preventing exploitation. However, if the Docker Model Runner is exposed to localhost over TCP in specific configurations, the vulnerability is still exploitable. | 2026-04-01 | 6.8 |
| CVE-2026-5164 | red hat - multiple products | A flaw was found in virtio-win. The `RhelDoUnMap()` function does not properly validate the number of descriptors provided by a user during an unmap request. A local user could exploit this input validation vulnerability by supplying an excessive number of descriptors, leading to a buffer overrun. This can cause a system crash, resulting in a Denial of Service (DoS). | 2026-03-30 | 6.7 |
| CVE-2026-5165 | red hat - multiple products | A flaw was found in virtio-win, specifically within the VirtIO Block (BLK) device. When the device undergoes a reset, it fails to properly manage memory, resulting in a use-after-free vulnerability. This issue could allow a local attacker to corrupt system memory, potentially leading to system instability or unexpected behavior. | 2026-03-30 | 6.7 |
| CVE-2026-34401 | microsoft - XmlNotepad | XML Notepad is a Windows program that provides a simple intuitive User Interface for browsing and editing XML documents. Prior to version 2.9.0.21, XML Notepad does not disable DTD processing by default which means external entities are resolved automatically. There is a well known attack related to malicious DTD files where an attacker to craft a malicious XML file that loads a DTD that causes XML Notepad to make outbound HTTP/SMB requests, potentially leaking local file contents or capturing the victim's NTLM credentials. This issue has been patched in version 2.9.0.21. | 2026-03-31 | 6.5 |
| CVE-2026-5276 | google - chrome | Insufficient policy enforcement in WebUSB in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High) | 2026-04-01 | 6.5 |
| CVE-2026-5283 | google - chrome | Inappropriate implementation in ANGLE in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High) | 2026-04-01 | 6.5 |
| CVE-2026-5291 | google - chrome | Inappropriate implementation in WebGL in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium) | 2026-04-01 | 6.5 |
| CVE-2026-20042 | cisco - Cisco Nexus Dashboard | A vulnerability in the configuration backup feature of Cisco Nexus Dashboard could allow an attacker who has the encryption password and access to Full or Config-only backup files to access sensitive information._x000D_ | 2026-04-01 | 6.5 |

| | | | | |
|---|---|---|---|---|
| | | _x000D_<br>This vulnerability exists because authentication details are included in the encrypted backup files. An attacker with a valid backup file and encryption password from an affected device could decrypt the backup file. The attacker could then use the authentication details in the backup file to access internal-only APIs on the affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system as the root user. | | |
| CVE-2026-20095 | cisco - multiple products | A vulnerability in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with admin-level privileges to perform command injection attacks on an affected system and execute arbitrary commands as the root user._x000D_<br>_x000D_<br>This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted commands to the web-based management interface of the affected software. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system as the root user. Cisco has assigned this vulnerability a Security Impact Rating (SIR) of High, rather than Medium as the score indicates, because additional security implications could occur once the attacker has become root. | 2026-04-01 | 6.5 |
| CVE-2026-20096 | cisco - multiple products | A vulnerability in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with admin-level privileges to perform command injection attacks on an affected system and execute arbitrary commands as the root user._x000D_<br>_x000D_<br>This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted commands to the web-based management interface of the affected software. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system as the root user. Cisco has assigned this vulnerability a Security Impact Rating (SIR) of High, rather than Medium as the score indicates, because additional security implications could occur once the attacker has become root. | 2026-04-01 | 6.5 |
| CVE-2026-20097 | cisco - Cisco Unified Computing System (Standalone) | A vulnerability in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with admin-level privileges to execute arbitrary code as the root user. This vulnerability is due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user._x000D_<br>_x000D_<br>Cisco has assigned this vulnerability a SIR of High rather than Medium as the score indicates because additional security implications could occur when the attacker becomes root. | 2026-04-01 | 6.5 |
| CVE-2025-36375 | ibm - multiple products | IBM DataPower Gateway 10.6CD 10.6.1.0 through 10.6.5.0 and IBM DataPower Gateway 10.5.0 10.5.0.0 through 10.5.0.20 and IBM DataPower Gateway 10.6.0 10.6.0.0 through 10.6.0.8 IBM DataPower Gateway is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. | 2026-04-01 | 6.5 |
| CVE-2026-5273 | google - chrome | Use after free in CSS in Google Chrome prior to 146.0.7680.178 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High) | 2026-04-01 | 6.3 |
| CVE-2025-66483 | ibm - aspera_shares | IBM Aspera Shares 1.9.9 through 1.11.0 does not invalidate session after a password reset which could allow an authenticated user to impersonate another user on the system. | 2026-04-01 | 6.3 |
| CVE-2025-43210 | apple - multiple products | An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in iOS 18.6 and iPadOS 18.6, iPadOS 17.7.9, macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7, tvOS 18.6, visionOS 2.6, watchOS 11.6. Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory. | 2026-04-02 | 6.3 |
| CVE-2025-43238 | apple - multiple products | An integer overflow was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to cause unexpected system termination. | 2026-04-02 | 6.2 |
| CVE-2026-20041 | cisco - multiple products | A vulnerability in Cisco Nexus Dashboard and Cisco Nexus Dashboard Insights could allow an unauthenticated, remote attacker to conduct a server-side request forgery (SSRF) attack through an affected device._x000D_<br>_x000D_<br>This vulnerability is due to improper input validation for specific HTTP requests. An attacker could exploit this vulnerability by persuading an authenticated user of the device management interface to click a crafted link. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected device to an attacker-controlled server. The attacker could then execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. | 2026-04-01 | 6.1 |
| CVE-2026-20085 | cisco - multiple products | A vulnerability in the web-based management interface of Cisco IMC could allow an unauthenticated, remote attacker to conduct a reflected XSS attack against a user of the interface._x000D_<br>_x000D_<br>This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the browser of the targeted user or access sensitive, browser-based information. | 2026-04-01 | 6.1 |
| CVE-2026-5170 | mongodb - multiple products | A user with access to the cluster with a limited set of privilege actions can trigger a crash of a mongod process during the limited and unpredictable window when the cluster is being promoted from a replica set to a sharded cluster. This may cause a denial of service by taking down the primary of the replica set.<br><br>This issue affects MongoDB Server v8.2 versions prior to 8.2.2, MongoDB Server v8.0 versions between 8.0.18, MongoDB Server v7.0 versions between 7.0.31. | 2026-03-30 | 6 |
| CVE-2025-13916 | ibm - aspera_shares | IBM Aspera Shares 1.9.9 through 1.11.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information | 2026-04-01 | 5.9 |

| | | | | |
|---|---|---|---|---|
| CVE-2025-66484 | ibm - aspera_shares | IBM Aspera Shares 1.9.9 through 1.11.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. | 2026-04-01 | 5.5 |
| CVE-2026-4364 | ibm - multiple products | IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 allows certificate listings retrieved via a browser session to return a JSON payload while incorrectly specifying the response Content-Type as text/html. Because the content is delivered with an HTML MIME type, browsers may interpret the JSON data as executable script under certain conditions. This creates an opportunity for JavaScript injection, potentially leading to cross-site scripting (XSS). | 2026-04-01 | 5.4 |
| CVE-2025-66485 | ibm - aspera_shares | IBM Aspera Shares 1.9.9 through 1.11.0 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. | 2026-04-01 | 5.4 |
| CVE-2026-1243 | ibm - multiple products | IBM Content Navigator 3.0.15, 3.1.0, and 3.2.0 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. | 2026-04-02 | 5.4 |
| CVE-2026-5183 | trendnet - TEW-713RE | A vulnerability was determined in TRENDnet TEW-713RE up to 1.02. The affected element is the function sub_421494 of the file /goform/addRouting. Executing a manipulation of the argument dest can lead to command injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-03-31 | 5.3 |
| CVE-2026-5184 | trendnet - TEW-713RE | A vulnerability was identified in TRENDnet TEW-713RE up to 1.02. The impacted element is an unknown function of the file /goform/setSysAdm. The manipulation of the argument admuser leads to command injection. The attack can be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-03-31 | 5.3 |
| CVE-2026-1491 | ibm - multiple products | IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 IBM Security Verify could allow a remote attacker to access sensitive information due to an inconsistent interpretation of an HTTP request by a reverse proxy. | 2026-04-01 | 5.3 |
| CVE-2026-2862 | ibm - multiple products | IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 IBM Security Verify could allow a remote attacker to access sensitive information due to an inconsistent interpretation of an HTTP request by a reverse proxy. | 2026-04-01 | 5.3 |
| CVE-2026-4325 | red hat - multiple products | A flaw was found in Keycloak. The SingleUseObjectProvider, a global key-value store, lacks proper type and namespace isolation. This vulnerability allows an attacker to delete arbitrary single-use entries, which can enable the replay of consumed action tokens, such as password reset links. This could lead to unauthorized access or account compromise. | 2026-04-02 | 5.3 |
| CVE-2026-5351 | trendnet - tew-657brm_firmware | A weakness has been identified in Trendnet TEW-657BRM 1.00.1. This affects the function add_wps_client of the file /setup.cgi. This manipulation of the argument wl_enrolee_pin causes os command injection. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor confirms, that "[t]he product in question (...) has been discontinued and end of life since June 23, 2011, that is more than 14 years ago. We no longer provide support for this product, so we are not able to confirm the vulnerabilities. We will make an announcement on our website's product support page and notify customers who registered their products with us." This vulnerability only affects products that are no longer supported by the maintainer. | 2026-04-02 | 5.3 |
| CVE-2026-5352 | trendnet - tew-657brm_firmware | A security vulnerability has been detected in Trendnet TEW-657BRM 1.00.1. This impacts the function Edit of the file /setup.cgi. Such manipulation of the argument pcdb_list leads to os command injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor confirms, that "[t]he product in question (...) has been discontinued and end of life since June 23, 2011, that is more than 14 years ago. We no longer provide support for this product, so we are not able to confirm the vulnerabilities. We will make an announcement on our website's product support page and notify customers who registered their products with us." This vulnerability only affects products that are no longer supported by the maintainer. | 2026-04-02 | 5.3 |
| CVE-2026-5353 | trendnet - tew-657brm_firmware | A vulnerability was detected in Trendnet TEW-657BRM 1.00.1. Affected is the function ping_test of the file /setup.cgi. Performing a manipulation of the argument c4_IPAddr results in os command injection. Remote exploitation of the attack is possible. The exploit is now public and may be used. The vendor confirms, that "[t]he product in question (...) has been discontinued and end of life since June 23, 2011, that is more than 14 years ago. We no longer provide support for this product, so we are not able to confirm the vulnerabilities. We will make an announcement on our website's product support page and notify customers who registered their products with us." This vulnerability only affects products that are no longer supported by the maintainer. | 2026-04-02 | 5.3 |
| CVE-2026-5354 | trendnet - tew-657brm_firmware | A flaw has been found in Trendnet TEW-657BRM 1.00.1. Affected by this vulnerability is the function vpn_connect of the file /setup.cgi. Executing a manipulation of the argument policy_name can lead to os command injection. The attack can be executed remotely. The exploit has been published and may be used. The vendor confirms, that "[t]he product in question (...) has been discontinued and end of life since June 23, 2011, that is more than 14 years ago. We no longer provide support for this product, so we are not able to confirm the vulnerabilities. We will make an announcement on our website's product support page and notify customers who registered their products with us." This vulnerability only affects products that are no longer supported by the maintainer. | 2026-04-02 | 5.3 |
| CVE-2026-5355 | trendnet - tew-657brm_firmware | A vulnerability has been found in Trendnet TEW-657BRM 1.00.1. Affected by this issue is the function vpn_drop of the file /setup.cgi. The manipulation of the argument policy_name leads to os command injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The vendor confirms, that "[t]he product in question (...) has been discontinued and end of life since June 23, 2011, that is more than 14 years ago. We no longer provide support for this product, so we are not able to confirm the vulnerabilities. We will make an announcement on our website's product support page and notify customers who registered their | 2026-04-02 | 5.3 |

| | | | | |
|---|---|---|---|---|
| | | products with us." This vulnerability only affects products that are no longer supported by the maintainer. | | |
| CVE-2026-20174 | cisco - multiple products | A vulnerability in the Metadata update feature of Cisco Nexus Dashboard Insights could allow an authenticated, remote attacker to write arbitrary files to an affected system._x000D_<br>_x000D_<br>This vulnerability is due to insufficient validation of the metadata update file. An attacker could exploit this vulnerability by crafting a metadata update file and manually uploading it to an affected device. A successful exploit could allow the attacker to write arbitrary files to the underlying operating system as the root user. To exploit this vulnerability, the attacker must have valid administrative credentials._x000D_<br>Note: Manual uploading of metadata files is typical for Air-Gap environments but not for Cisco Intersight Cloud connected devices. However, the manual upload option exists for both deployments. | 2026-04-01 | 4.9 |
| CVE-2026-32794 | apache - airflow_providers_databricks | Improper Certificate Validation vulnerability in Apache Airflow Provider for Databricks. Provider code did not validate certificates for connections to Databricks back-end which could result in a man-of-a-middle attack that traffic is intercepted and manipulated or credentials exfiltrated w/o notice.<br><br>This issue affects Apache Airflow Provider for Databricks: from 1.10.0 before 1.12.0.<br><br>Users are recommended to upgrade to version 1.12.0, which fixes the issue. | 2026-03-30 | 4.8 |
| CVE-2026-3468 | sonicwall - Email Security | A stored Cross-Site Scripting (XSS) vulnerability has been identified in the SonicWall Email Security appliance due to improper neutralization of user-supplied input during web page generation, allowing a remote authenticated attacker as admin user to potentially execute arbitrary JavaScript code. | 2026-03-31 | 4.8 |
| CVE-2026-20087 | cisco - multiple products | A vulnerability in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with administrative privileges to conduct a stored XSS attack against a user of the interface._x000D_<br>_x000D_<br>This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the browser of the targeted user or access sensitive, browser-based information. | 2026-04-01 | 4.8 |
| CVE-2026-20088 | cisco - multiple products | A vulnerability in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with administrative privileges to conduct a stored XSS attack against a user of the interface._x000D_<br>_x000D_<br>This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the browser of the targeted user or access sensitive, browser-based information. | 2026-04-01 | 4.8 |
| CVE-2026-20089 | cisco - multiple products | A vulnerability in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with administrative privileges to conduct a stored XSS attack against a user of the interface._x000D_<br>_x000D_<br>This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the browser of the targeted user or access sensitive, browser-based information. | 2026-04-01 | 4.8 |
| CVE-2026-20090 | cisco - multiple products | A vulnerability in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with administrative privileges to conduct a stored XSS attack against a user of the interface._x000D_<br>_x000D_<br>This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the browser of the targeted user or access sensitive, browser-based information. | 2026-04-01 | 4.8 |
| CVE-2025-66486 | ibm - aspera_shares | IBM Aspera Shares 1.9.9 through 1.11.0 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. | 2026-04-01 | 4.8 |
| CVE-2026-27101 | dell - multiple products | Dell Secure Connect Gateway (SCG) 5.0 Appliance and Application version(s) 5.28.00.xx to 5.32.00.xx, contain(s) an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability. A high privileged attacker within the management network could potentially exploit this vulnerability, leading to remote execution. | 2026-04-01 | 4.7 |
| CVE-2026-28265 | dell - powerstoreos | PowerStore, contains a Path Traversal vulnerability in the Service user. A low privileged attacker with local access could potentially exploit this vulnerability, leading to modification of arbitrary system files. | 2026-04-01 | 4.4 |
| CVE-2026-4820 | ibm - multiple products | IBM Maximo Application Suite 9.1, 9.0, 8.11, and 8.10 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. | 2026-04-01 | 4.3 |
| CVE-2026-35414 | openbsd - openssh | OpenSSH before 10.3 mishandles the authorized_keys principals option in uncommon scenarios involving a principals list in conjunction with a Certificate Authority that makes certain use of comma characters. | 2026-04-02 | 4.2 |
| CVE-2025-36373 | ibm - multiple products | IBM DataPower Gateway 10.6CD 10.6.1.0 through 10.6.5.0 and IBM DataPower Gateway 10.5.0 10.5.0.0 through 10.5.0.20 and IBM DataPower Gateway 10.6.0 10.6.0.0 through 10.6.0.8 IBM DataPower Gateway could disclose sensitive system information from other domains to an administrative user. | 2026-04-01 | 4.1 |

| | | | | |
|---|---|---|---|---|
| CVE-2026-2625 | red hat - multiple products | A flaw was found in rust-rpm-sequoia. An attacker can exploit this vulnerability by providing a specially crafted Red Hat Package Manager (RPM) file. During the RPM signature verification process, this crafted file can trigger an error in the OpenPGP signature parsing code, leading to an unconditional termination of the rpm process. This issue results in an application level denial of service, making the system unable to process RPM files for signature verification. | 2026-04-03 | 4 |
| CVE-2026-3470 | sonicwall - Email Security | A vulnerability exists in the SonicWall Email Security appliance due to improper input sanitization that may lead to data corruption, allowing a remote authenticated attacker as admin user could exploit this issue by providing crafted input that corrupts application database. | 2026-03-31 | 3.8 |
| CVE-2026-3184 | red hat - multiple products | A flaw was found in util-linux. Improper hostname canonicalization in the `login(1)` utility, when invoked with the `-h` option, can modify the supplied remote hostname before setting `PAM_RHOST`. A remote attacker could exploit this by providing a specially crafted hostname, potentially bypassing host-based Pluggable Authentication Modules (PAM) access control rules that rely on fully qualified domain names. This could lead to unauthorized access. | 2026-04-03 | 3.7 |
| CVE-2026-35386 | openbsd - OpenSSH | In OpenSSH before 10.3, command execution can occur via shell metacharacters in a username within a command line. This requires a scenario where the username on the command line is untrusted, and also requires a non-default configurations of % in ssh_config. | 2026-04-02 | 3.6 |
| CVE-2025-43236 | apple - multiple products | A type confusion issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An attacker may be able to cause unexpected app termination. | 2026-04-02 | 3.3 |
| CVE-2026-2475 | ibm - multiple products | IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 could allow a remote attacker to conduct phishing attacks, caused by an open redirect vulnerability. An attacker could exploit this vulnerability using a specially crafted request to redirect a victim to arbitrary Web sites. | 2026-04-01 | 3.1 |
| CVE-2026-35387 | openbsd - OpenSSH | OpenSSH before 10.3 can use unintended ECDSA algorithms. Listing of any ECDSA algorithm in PubkeyAcceptedAlgorithms or HostbasedAcceptedAlgorithms is misinterpreted to mean all ECDSA algorithms. | 2026-04-02 | 3.1 |
| CVE-2026-3469 | sonicwall - Email Security | A denial-of-service (DoS) vulnerability exists due to improper input validation in the SonicWall Email Security appliance, allowing a remote authenticated attacker as admin user to cause the application to become unresponsive. | 2026-03-31 | 2.7 |
| CVE-2025-66487 | ibm - aspera_shares | IBM Aspera Shares 1.9.9 through 1.11.0 does not properly rate limit the frequency that an authenticated user can send emails, which could result in email flooding or a denial of service. | 2026-04-01 | 2.7 |
| CVE-2026-35388 | openbsd - OpenSSH | OpenSSH before 10.3 omits connection multiplexing confirmation for proxy-mode multiplexing sessions. | 2026-04-02 | 2.5 |
| 140 | | | | |
| 141 | | | | |
| 142 | | | | |
| 143 | | | | |
| 144 | | | | |
| 145 | | | | |
| 146 | | | | |
| 147 | | | | |
| 148 | | | | |
| 149 | | | | |
| 150 | | | | |
| 151 | | | | |
| 152 | | | | |
| 153 | | | | |
| 154 | | | | |
| 155 | | | | |
| 156 | | | | |
| 157 | | | | |
| 158 | | | | |
| 159 | | | | |
| 160 | | | | |
| 161 | | | | |
| 162 | | | | |
| 163 | | | | |
| 164 | | | | |
| 165 | | | | |
| 166 | | | | |
| 167 | | | | |
| 168 | | | | |
| 169 | | | | |
| 170 | | | | |
| 171 | | | | |
| 172 | | | | |
| 173 | | | | |
| 174 | | | | |
| 175 | | | | |
| 176 | | | | |
| 177 | | | | |
| 178 | | | | |
| 179 | | | | |
| 180 | | | | |
| 181 | | | | |
| 182 | | | | |
| 183 | | | | |

| | | | | |
|---|---|---|---|---|
| 184 | | | | |
| 185 | | | | |
| 186 | | | | |
| 187 | | | | |
| 188 | | | | |
| 189 | | | | |
| 190 | | | | |
| 191 | | | | |
| 192 | | | | |
| 193 | | | | |
| 194 | | | | |
| 195 | | | | |
| 196 | | | | |
| 197 | | | | |
| 198 | | | | |
| 199 | | | | |
| 200 | | | | |
| 201 | | | | |
| 202 | | | | |
| 203 | | | | |
| 204 | | | | |
| 205 | | | | |
| 206 | | | | |
| 207 | | | | |
| 208 | | | | |
| 209 | | | | |
| 210 | | | | |
| 211 | | | | |
| 212 | | | | |
| 213 | | | | |
| 214 | | | | |
| 215 | | | | |
| 216 | | | | |
| 217 | | | | |
| 218 | | | | |
| 219 | | | | |
| 220 | | | | |
| 221 | | | | |
| 222 | | | | |
| 223 | | | | |
| 224 | | | | |
| 225 | | | | |
| 226 | | | | |
| 227 | | | | |
| 228 | | | | |
| 229 | | | | |
| 230 | | | | |
| 231 | | | | |
| 232 | | | | |
| 233 | | | | |
| 234 | | | | |
| 235 | | | | |
| 236 | | | | |
| 237 | | | | |
| 238 | | | | |
| 239 | | | | |
| 240 | | | | |
| 241 | | | | |
| 242 | | | | |
| 243 | | | | |
| 244 | | | | |
| 245 | | | | |
| 246 | | | | |
| 247 | | | | |
| 248 | | | | |
| 249 | | | | |
| 250 | | | | |
| 251 | | | | |
| 252 | | | | |
| 253 | | | | |
| 254 | | | | |
| 255 | | | | |
| 256 | | | | |
| 257 | | | | |
| 258 | | | | |
| 259 | | | | |
| 260 | | | | |

| | | | | |
|---|---|---|---|---|
| 261 | | | | |
| 262 | | | | |
| 263 | | | | |
| 264 | | | | |
| 265 | | | | |
| 266 | | | | |
| 267 | | | | |
| 268 | | | | |
| 269 | | | | |
| 270 | | | | |
| 271 | | | | |
| 272 | | | | |
| 273 | | | | |
| 274 | | | | |
| 275 | | | | |
| 276 | | | | |
| 277 | | | | |
| 278 | | | | |
| 279 | | | | |
| 280 | | | | |
| 281 | | | | |
| 282 | | | | |
| 283 | | | | |
| 284 | | | | |
| 285 | | | | |
| 286 | | | | |
| 287 | | | | |
| 288 | | | | |
| 289 | | | | |
| 290 | | | | |
| 290 | | | | |
| 291 | | | | |
| 292 | | | | |
| 293 | | | | |
| 294 | | | | |
| 295 | | | | |
| 296 | | | | |
| 297 | | | | |
| 298 | | | | |

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.

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.