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 22 مارس إلى 28 مارس. 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 22nd of March to 28th of March. 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-2026-4688	mozilla - multiple products	Sandbox escape due to use-after-free in the Disability Access APIs component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	10
CVE-2026-4689	mozilla - multiple products	Sandbox escape due to incorrect boundary conditions, integer overflow in the XPCOM component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	10
CVE-2026-4692	mozilla - multiple products	Sandbox escape in the Responsive Design Mode component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	10
CVE-2026-4725	mozilla - firefox	Sandbox escape due to use-after-free in the Graphics: Canvas2D component. This vulnerability affects Firefox < 149 and Thunderbird < 149.	2026-03-24	10
CVE-2026-4691	mozilla - multiple products	Use-after-free in the CSS Parsing and Computation component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	9.8
CVE-2026-4696	mozilla - multiple products	Use-after-free in the Layout: Text and Fonts component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	9.8
CVE-2026-4698	mozilla - multiple products	JIT miscompilation in the JavaScript Engine: JIT component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	9.8
CVE-2026-4700	mozilla - multiple products	Mitigation bypass in the Networking: HTTP component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	9.8
CVE-2026-4701	mozilla - multiple products	Use-after-free in the JavaScript Engine component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	9.8
CVE-2026-4702	mozilla - multiple products	JIT miscompilation in the JavaScript Engine component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	9.8
CVE-2026-4705	mozilla - multiple products	Undefined behavior in the WebRTC: Signaling component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	9.8
CVE-2026-4710	mozilla - multiple products	Incorrect boundary conditions in the Audio/Video component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	9.8
CVE-2026-4711	mozilla - multiple products	Use-after-free in the Widget: Cocoa component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	9.8
CVE-2026-4717	mozilla - multiple products	Privilege escalation in the Netmonitor component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	9.8
CVE-2026-4720	mozilla - multiple products	Memory safety bugs present in Firefox ESR 140.8, Thunderbird ESR 140.8, Firefox 148 and Thunderbird 148. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	9.8
CVE-2026-4721	mozilla - multiple products	Memory safety bugs present in Firefox ESR 115.33, Firefox ESR 140.8, Thunderbird ESR 140.8, Firefox 148 and Thunderbird 148. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	9.8
CVE-2026-4723	mozilla - firefox	Use-after-free in the JavaScript Engine component. This vulnerability affects Firefox < 149 and Thunderbird < 149.	2026-03-24	9.8
CVE-2026-4729	mozilla - multiple products	Memory safety bugs present in Firefox 148 and Thunderbird 148. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 149 and Thunderbird < 149.	2026-03-24	9.8

CVE-2026-28858	apple - multiple products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 26.4 and iPadOS 26.4. A remote user may be able to cause unexpected system termination or corrupt kernel memory.	2026-03-25	9.8
CVE-2026-3055	citrix - multiple products	Insufficient input validation in NetScaler ADC and NetScaler Gateway when configured as a SAML IDP leading to memory overread	2026-03-23	9.3
CVE-2026-20688	apple - multiple products	A path handling issue was addressed with improved validation. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, visionOS 26.4. An app may be able to break out of its sandbox.	2026-03-25	9.3
CVE-2026-28827	apple - multiple products	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to break out of its sandbox.	2026-03-25	9.3
CVE-2026-4715	mozilla - multiple products	Uninitialized memory in the Graphics: Canvas2D component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	9.1
CVE-2026-4716	mozilla - multiple products	Incorrect boundary conditions, uninitialized memory in the JavaScript Engine component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	9.1
CVE-2026-4724	mozilla - multiple products	Undefined behavior in the Audio/Video component. This vulnerability affects Firefox < 149 and Thunderbird < 149.	2026-03-24	9.1
CVE-2026-27876	grafana - multiple products	A chained attack via SQL Expressions and a Grafana Enterprise plugin can lead to a remote arbitrary code execution impact (RCE). This is enabled by a feature in Grafana (OSS), so all users are always recommended to update to avoid future attack vectors going this path. Only instances with the sqlExpressions feature toggle enabled are vulnerable. Only instances in the following version ranges are affected: - 11.6.0 (inclusive) to 11.6.14 (exclusive): 11.6.14 has the fix. 11.5 and below are not affected. - 12.0.0 (inclusive) to 12.1.10 (exclusive): 12.1.10 has the fix. 12.0 did not receive an update, as it is end-of-life. - 12.2.0 (inclusive) to 12.2.8 (exclusive): 12.2.8 has the fix. - 12.3.0 (inclusive) to 12.3.6 (exclusive): 12.3.6 has the fix. - 12.4.0 (inclusive) to 12.4.2 (exclusive): 12.4.2 has the fix. 13.0.0 and above also have the fix: no v13 release is affected.	2026-03-27	9.1
CVE-2026-33765	pi-hole - web	Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level ad and internet tracker blocking application. Versions prior to 6.0 have a critical OS Command Injection vulnerability in the savesettings.php file. The application takes the user-controlled $_POST['webtheme'] parameter and concatenates it directly into a system command executed via PHP's exec() function. Since the input is neither sanitized nor validated before being passed to the shell, an attacker can append arbitrary system commands to the intended pihole command. Furthermore, because the command is executed with sudo privileges, the injected commands will run with elevated (likely root) privileges. Version 6.0 patches the issue.	2026-03-27	8.9
CVE-2026-4673	google - chrome	Heap buffer overflow in WebAudio in Google Chrome prior to 146.0.7680.165 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	2026-03-24	8.8
CVE-2026-4674	google - chrome	Out of bounds read in CSS in Google Chrome prior to 146.0.7680.165 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	2026-03-24	8.8
CVE-2026-4675	google - chrome	Heap buffer overflow in WebGL in Google Chrome prior to 146.0.7680.165 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	2026-03-24	8.8
CVE-2026-4676	google - chrome	Use after free in Dawn in Google Chrome prior to 146.0.7680.165 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-03-24	8.8
CVE-2026-4677	google - chrome	Inappropriate implementation in WebAudio in Google Chrome prior to 146.0.7680.165 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	2026-03-24	8.8
CVE-2026-4678	google - chrome	Use after free in WebGPU in Google Chrome prior to 146.0.7680.165 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-03-24	8.8
CVE-2026-4679	google - chrome	Integer overflow in Fonts in Google Chrome prior to 146.0.7680.165 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	2026-03-24	8.8
CVE-2026-4680	google - chrome	Use after free in FedCM in Google Chrome prior to 146.0.7680.165 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-03-24	8.8
CVE-2026-4722	mozilla - firefox	Privilege escalation in the IPC component. This vulnerability affects Firefox < 149 and Thunderbird < 149.	2026-03-24	8.8
CVE-2026-27654	f5 - multiple products	NGINX Open Source and NGINX Plus have a vulnerability in the ngx_http_dav_module module that might allow an attacker to trigger a buffer overflow to the NGINX worker process; this vulnerability may result in termination of the NGINX worker process or modification of source or destination file names outside the document root. This issue affects NGINX Open Source and NGINX Plus when the configuration file uses DAV module MOVE or COPY methods, prefix location (nonregular expression location configuration), and alias directives. The integrity impact is constrained because the NGINX worker process user has low privileges and does not have access to the entire system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-03-24	8.8
CVE-2026-20631	apple - macos	A logic issue was addressed with improved checks. This issue is fixed in macOS Tahoe 26.4. A user may be able to elevate privileges.	2026-03-25	8.8
CVE-2026-23395	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix accepting multiple L2CAP_ECRED_CONN_REQ Currently the code attempts to accept requests regardless of the	2026-03-25	8.8

		command identifier which may cause multiple requests to be marked as pending (FLAG_DEFER_SETUP) which can cause more than L2CAP_ECRED_MAX_CID(5) to be allocated in l2cap_ecred_rsp_defer causing an overflow. The spec is quite clear that the same identifier shall not be used on subsequent requests: 'Within each signaling channel a different Identifier shall be used for each successive request or indication.' https://www.bluetooth.com/wp-content/uploads/Files/Specification/HTML/Core-62/out/en/host/logical-link-control-and-adaptation-protocol-specification.html#UUID-32a25a06-4aa4-c6c7-77c5-dcfe3682355d So this attempts to check if there are any channels pending with the same identifier and rejects if any are found.		
CVE-2026-27651	f5 - multiple products	When the ngx_mail_auth_http_module module is enabled on NGINX Plus or NGINX Open Source, undisclosed requests can cause worker processes to terminate. This issue may occur when (1) CRAM-MD5 or APOP authentication is enabled, and (2) the authentication server permits retry by returning the Auth-Wait response header. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-03-24	8.7
CVE-2026-23921	zabbix - Zabbix	A low privilege Zabbix user with API access can exploit a blind SQL injection vulnerability in include/classes/api/CApiService.php to execute arbitrary SQL selects via the sortfield parameter. Although query results are not returned directly, an attacker can exfiltrate arbitrary database data through time-based techniques, potentially leading to session identifier disclosure and administrator account compromise.	2026-03-24	8.7
CVE-2026-27664	siemens - multiple products	A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V26.10), SICORE Base system (All versions < V26.10.0). The affected application contains an out-of-bounds write vulnerability while parsing specially crafted XML inputs. This could allow an unauthenticated attacker to exploit this issue by sending a malicious XML request, which may cause the service to crash, resulting in a denial-of-service condition.	2026-03-26	8.7
CVE-2026-28367	red hat - multiple products	A flaw was found in Undertow. A remote attacker can exploit this vulnerability by sending `\r\r\r` as a header block terminator. This can be used for request smuggling with certain proxy servers, such as older versions of Apache Traffic Server and Google Cloud Classic Application Load Balancer, potentially leading to unauthorized access or manipulation of web requests.	2026-03-27	8.7
CVE-2026-28368	redhat - multiple products	A flaw was found in Undertow. This vulnerability allows a remote attacker to construct specially crafted requests where header names are parsed differently by Undertow compared to upstream proxies. This discrepancy in header interpretation can be exploited to launch request smuggling attacks, potentially bypassing security controls and accessing unauthorized resources.	2026-03-27	8.7
CVE-2026-28369	redhat - multiple products	A flaw was found in Undertow. When Undertow receives an HTTP request where the first header line starts with one or more spaces, it incorrectly processes the request by stripping these leading spaces. This behavior, which violates HTTP standards, can be exploited by a remote attacker to perform request smuggling. Request smuggling allows an attacker to bypass security mechanisms, access restricted information, or manipulate web caches, potentially leading to unauthorized actions or data exposure.	2026-03-27	8.7
CVE-2025-15517	tp-link - archer_nx600_firmware	A missing authentication check in the HTTP server on TP-Link Archer NX200, NX210, NX500 and NX600 to certain cgi endpoints allows unauthenticated access intended for authenticated users. An attacker may perform privileged HTTP actions without authentication, including firmware upload and configuration operations.	2026-03-23	8.6
CVE-2026-4627	d-link - multiple products	A vulnerability was found in D-Link DIR-825 and DIR-825R 1.0.5/4.5.1. Affected is the function handler_update_system_time of the file libdeuteron_modules.so of the component NTP Service. The manipulation results in os command injection. The attack may be launched remotely. This vulnerability only affects products that are no longer supported by the maintainer.	2026-03-24	8.6
CVE-2026-4687	mozilla - multiple products	Sandbox escape due to incorrect boundary conditions in the Telemetry component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	8.6
CVE-2026-4690	mozilla - multiple products	Sandbox escape due to incorrect boundary conditions, integer overflow in the XPCOM component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	8.6
CVE-2026-20012	cisco - multiple products	A vulnerability in the Internet Key Exchange version 2 (IKEv2) feature of Cisco IOS Software, Cisco IOS XE Software, Cisco Secure Firewall Adaptive Security Appliance (ASA) Software, and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a memory leak, resulting in a denial of service (DoS) condition on an affected device._x000D_ _x000D_ This vulnerability is due to improper parsing of IKEv2 packets. An attacker could exploit this vulnerability by sending crafted IKEv2 packets to an affected device. A successful exploit of Cisco IOS Software and IOS XE Software could allow the attacker to cause the affected device to reload, resulting in a DoS condition. A successful exploit of Cisco Secure Firewall ASA Software and Secure FTD Software could allow the attacker to partially exhaust system memory, resulting in system instability, such as the inability to establish new IKEv2 VPN sessions. A manual reboot of the device is required to recover from this condition.	2026-03-25	8.6
CVE-2026-20084	cisco - Cisco IOS XE Software	A vulnerability in the DHCP snooping feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause BOOTP packets to be forwarded between VLANs, resulting in a denial of service (DoS) condition. _x000D_ _x000D_ This vulnerability is due to improper handling of BOOTP packets on Cisco Catalyst 9000 Series Switches. An attacker could exploit this vulnerability by sending BOOTP request packets to an affected device. A successful exploit could allow an attacker to forward BOOTP packets from one VLAN to another, resulting in BOOTP VLAN leakage and potentially leading to high CPU utilization. This makes the device unreachable (either through console or remote management) and unable to forward traffic, resulting in a DoS condition. _x000D_	2026-03-25	8.6

		_x000D_ Note: This vulnerability can be exploited with either unicast or broadcast BOOTP packets._x000D_ _x000D_ There are workarounds that address this vulnerability.		
CVE-2026-20086	cisco - Cisco IOS XE Software	A vulnerability in the processing of Control and Provisioning of Wireless Access Points (CAPWAP) packets of Cisco IOS XE Wireless Controller Software for the Catalyst CW9800 Family could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device._x000D_ _x000D_ This vulnerability is due to improper handling of a malformed CAPWAP packet. An attacker could exploit this vulnerability by sending a malformed CAPWAP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload unexpectedly, resulting in a DoS condition.	2026-03-25	8.6
CVE-2025-15518	tp-link - archer_nx600_firmware	Improper input handling in a wireless-control administrative CLI command on TP-Link Archer NX200, NX210, NX500 and NX600 allows crafted input to be executed as part of an operating system command. An authenticated attacker with administrative privileges may execute arbitrary commands on the operating system, impacting the confidentiality, integrity, and availability of the device.	2026-03-23	8.5
CVE-2025-15519	tp-link - archer_nx600_firmware	Improper input handling in a modem-management administrative CLI command on TP-Link Archer NX200, NX210, NX500 and NX600 allows crafted input to be executed as part of an operating system command. An authenticated attacker with administrative privileges may execute arbitrary commands on the operating system, impacting the confidentiality, integrity, and availability of the device.	2026-03-23	8.5
CVE-2025-15605	tp-link - archer_nx600_firmware	A hardcoded cryptographic key within the configuration mechanism on TP-Link Archer NX200, NX210, NX500 and NX600 enables decryption and re-encryption of device configuration data. An authenticated attacker may decrypt configuration files, modify them, and re-encrypt them, affecting the confidentiality and integrity of device configuration data.	2026-03-23	8.5
CVE-2026-27784	f5 - multiple products	The 32-bit implementation of NGINX Open Source has a vulnerability in the ngx_http_mp4_module module, which might allow an attacker to over-read or over-write NGINX worker memory resulting in its termination, using a specially crafted MP4 file. The issue only affects 32-bit NGINX Open Source if it is built with the ngx_http_mp4_module module and the mp4 directive is used in the configuration file. Additionally, the attack is possible only if an attacker can trigger the processing of a specially crafted MP4 file with the ngx_http_mp4_module module. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-03-24	8.5
CVE-2026-32647	f5 - multiple products	NGINX Open Source and NGINX Plus have a vulnerability in the ngx_http_mp4_module module, which might allow an attacker to trigger a buffer over-read or over-write to the NGINX worker memory resulting in its termination or possibly code execution, using a specially crafted MP4 file. This issue affects NGINX Open Source and NGINX Plus if it is built with the ngx_http_mp4_module module and the mp4 directive is used in the configuration file. Additionally, the attack is possible only if an attacker can trigger the processing of a specially crafted MP4 file with the ngx_http_mp4_module module. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-03-24	8.5
CVE-2026-28821	apple - multiple products	A validation issue existed in the entitlement verification. This issue was addressed with improved validation of the process entitlement. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to gain elevated privileges.	2026-03-25	8.4
CVE-2026-28832	apple - multiple products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to disclose kernel memory.	2026-03-25	8.4
CVE-2026-31788	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: xen/privcmd: restrict usage in unprivileged domU The Xen privcmd driver allows to issue arbitrary hypercalls from user space processes. This is normally no problem, as access is usually limited to root and the hypervisor will deny any hypercalls affecting other domains. In case the guest is booted using secure boot, however, the privcmd driver would be enabling a root user process to modify e.g. kernel memory contents, thus breaking the secure boot feature. The only known case where an unprivileged domU is really needing to use the privcmd driver is the case when it is acting as the device model for another guest. In this case all hypercalls issued via the privcmd driver will target that other guest. Fortunately the privcmd driver can already be locked down to allow only hypercalls targeting a specific domain, but this mode can be activated from user land only today. The target domain can be obtained from Xenstore, so when not running in dom0 restrict the privcmd driver to that target domain from the beginning, resolving the potential problem of breaking secure boot. This is XSA-482 --- V2:	2026-03-25	8.2

		- defer reading from Xenstore if Xenstore isn't ready yet (Jan Beulich) - wait in open() if target domain isn't known yet - issue message in case no target domain found (Jan Beulich)		
CVE-2026-4718	mozilla - multiple products	Undefined behavior in the WebRTC: Signaling component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	8.1
CVE-2026-28817	apple - multiple products	A race condition was addressed with improved state handling. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. A sandboxed process may be able to circumvent sandbox restrictions.	2026-03-25	8.1
CVE-2026-28891	apple - multiple products	A race condition was addressed with additional validation. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to break out of its sandbox.	2026-03-25	8.1
CVE-2025-12805	red hat - multiple products	A flaw was found in Red Hat OpenShift AI (RHOAI) llama-stack-operator. This vulnerability allows unauthorized access to Llama Stack services deployed in other namespaces via direct network requests, because no NetworkPolicy restricts access to the llama-stack service endpoint. As a result, a user in one namespace can access another user’s Llama Stack instance and potentially view or manipulate sensitive data.	2026-03-26	8.1
CVE-2026-1961	red hat - multiple products	A flaw was found in Foreman. A remote attacker could exploit a command injection vulnerability in Foreman's WebSocket proxy implementation. This vulnerability arises from the system's use of unsanitized hostname values from compute resource providers when constructing shell commands. By operating a malicious compute resource server, an attacker could achieve remote code execution on the Foreman server when a user accesses VM VNC console functionality. This could lead to the compromise of sensitive credentials and the entire managed infrastructure.	2026-03-26	8
CVE-2026-4775	red hat - multiple products	A flaw was found in the libtiff library. A remote attacker could exploit a signed integer overflow vulnerability in the putcontig8bitYCbCr44tile function by providing a specially crafted TIFF file. This flaw can lead to an out-of-bounds heap write due to incorrect memory pointer calculations, potentially causing a denial of service (application crash) or arbitrary code execution.	2026-03-24	7.8
CVE-2026-20698	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. An app may be able to cause unexpected system termination or corrupt kernel memory.	2026-03-25	7.8
CVE-2026-23280	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Prevent ubuf size overflow The ubuf size calculation may overflow, resulting in an undersized allocation and possible memory corruption. Use check_add_overflow() helpers to validate the size calculation before allocation.	2026-03-25	7.8
CVE-2026-23288	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Fix out-of-bounds memset in command slot handling The remaining space in a command slot may be smaller than the size of the command header. Clearing the command header with memset() before verifying the available slot space can result in an out-of-bounds write and memory corruption. Fix this by moving the memset() call after the size validation.	2026-03-25	7.8
CVE-2026-23306	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: scsi: pm8001: Fix use-after-free in pm8001_queue_command() Commit e29c47fe8946 ("scsi: pm8001: Simplify pm8001_task_exec()") refactors pm8001_queue_command(), however it introduces a potential cause of a double free scenario when it changes the function to return -ENODEV in case of phy down/device gone state. In this path, pm8001_queue_command() updates task status and calls task_done to indicate to upper layer that the task has been handled. However, this also frees the underlying SAS task. A -ENODEV is then returned to the caller. When libsas sas_ata_qc_issue() receives this error value, it assumes the task wasn't handled/queued by LLDD and proceeds to clean up and free the task again, resulting in a double free. Since pm8001_queue_command() handles the SAS task in this case, it should return 0 to the caller indicating that the task has been handled.	2026-03-25	7.8
CVE-2026-23317	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: Return the correct value in vmw_translate_ptr functions Before the referenced fixes these functions used a lookup function that returned a pointer. This was changed to another lookup function that returned an error code with the pointer becoming an out parameter. The error path when the lookup failed was not changed to reflect this change and the code continued to return the PTR_ERR of the now uninitialized pointer. This could cause the vmw_translate_ptr functions to return success when they actually failed causing further uninitialized and OOB accesses.	2026-03-25	7.8

CVE-2026-23336	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: cancel rfkill_block work in wiphy_unregister() There is a use-after-free error in cfg80211_shutdown_all_interfaces found by syzkaller: BUG: KASAN: use-after-free in cfg80211_shutdown_all_interfaces+0x213/0x220 Read of size 8 at addr ffff888112a78d98 by task kworker/0:5/5326 CPU: 0 UID: 0 PID: 5326 Comm: kworker/0:5 Not tainted 6.19.0-rc2 #2 PREEMPT(voluntary) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Workqueue: events cfg80211_rfkill_block_work Call Trace: <TASK> dump_stack_lvl+0x116/0x1f0 print_report+0xcd/0x630 kasan_report+0xe0/0x110 cfg80211_shutdown_all_interfaces+0x213/0x220 cfg80211_rfkill_block_work+0x1e/0x30 process_one_work+0x9cf/0x1b70 worker_thread+0x6c8/0xf10 kthread+0x3c5/0x780 ret_from_fork+0x56d/0x700 ret_from_fork_asm+0x1a/0x30 </TASK> The problem arises due to the rfkill_block work is not cancelled when wiphy is being unregistered. In order to fix the issue cancel the corresponding work in wiphy_unregister(). Found by Linux Verification Center (linuxtesting.org) with Syzkaller.	2026-03-25	7.8
CVE-2026-23340	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net: sched: avoid qdisc_reset_all_tx_gt() vs dequeue race for lockless qdiscs When shrinking the number of real tx queues, netif_set_real_num_tx_queues() calls qdisc_reset_all_tx_gt() to flush qdiscs for queues which will no longer be used. qdisc_reset_all_tx_gt() currently serializes qdisc_reset() with qdisc_lock(). However, for lockless qdiscs, the dequeue path is serialized by qdisc_run_begin/end() using qdisc->seqlock instead, so qdisc_reset() can run concurrently with __qdisc_run() and free skbs while they are still being dequeued, leading to UAF. This can easily be reproduced on e.g. virtio-net by imposing heavy traffic while frequently changing the number of queue pairs: iperf3 -ub0 -c $peer -t 0 & while :; do ethtool -L eth0 combined 1 ethtool -L eth0 combined 2 done With KASAN enabled, this leads to reports like: BUG: KASAN: slab-use-after-free in __qdisc_run+0x133f/0x1760 ... Call Trace: <TASK> ... __qdisc_run+0x133f/0x1760 __dev_queue_xmit+0x248f/0x3550 ip_finish_output2+0xa42/0x2110 ip_output+0x1a7/0x410 ip_send_skb+0x2e6/0x480 udp_send_skb+0xb0a/0x1590 udp_sendmsg+0x13c9/0x1fc0 ... </TASK> Allocated by task 1270 on cpu 5 at 44.558414s: ... alloc_skb_with_frags+0x84/0x7c0 sock_alloc_send_pskb+0x69a/0x830 __ip_append_data+0x1b86/0x48c0 ip_make_skb+0x1e8/0x2b0 udp_sendmsg+0x13a6/0x1fc0 ...	2026-03-25	7.8

		Freed by task 1306 on cpu 3 at 44.558445s: ... kmem_cache_free+0x117/0x5e0 pfifo_fast_reset+0x14d/0x580 qdisc_reset+0x9e/0x5f0 netif_set_real_num_tx_queues+0x303/0x840 virtnet_set_channels+0x1bf/0x260 [virtio_net] ethnl_set_channels+0x684/0xae0 ethnl_default_set_doit+0x31a/0x890 ... Serialize qdisc_reset_all_tx_gt() against the lockless dequeue path by taking qdisc->seqlock for TCQ_F_NOLOCK qdiscs, matching the serialization model already used by dev_reset_queue(). Additionally clear QDISC_STATE_NON_EMPTY after reset so the qdisc state reflects an empty queue, avoiding needless re-scheduling.		
CVE-2026-23350	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/xe/queue: Call fini on exec queue creation fail Every call to queue init should have a corresponding fini call. Skipping this would mean skipping removal of the queue from GuC list (which is part of guc_id allocation). A damaged queue stored in exec_queue_lookup list would lead to invalid memory reference, sooner or later. Call fini to free guc_id. This must be done before any internal LRCs are freed. Since the finalization with this extra call became very similar to __xe_exec_queue_fini(), reuse that. To make this reuse possible, alter xe_lrc_put() so it can survive NULL parameters, like other similar functions. v2: Reuse _xe_exec_queue_fini(). Make xe_lrc_put() aware of NULLs. (cherry picked from commit 393e5fea6f7d7054abc2c3d97a4cfe8306cd6079)	2026-03-25	7.8
CVE-2026-23351	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_set_pipapo: split gc into unlink and reclaim phase Yiming Qian reports Use-after-free in the pipapo set type: Under a large number of expired elements, commit-time GC can run for a very long time in a non-preemptible context, triggering soft lockup warnings and RCU stall reports (local denial of service). We must split GC in an unlink and a reclaim phase. We cannot queue elements for freeing until pointers have been swapped. Expired elements are still exposed to both the packet path and userspace dumpers via the live copy of the data structure. call_rcu() does not protect us: dump operations or element lookups starting after call_rcu has fired can still observe the free'd element, unless the commit phase has made enough progress to swap the clone and live pointers before any new reader has picked up the old version. This a similar approach as done recently for the rbtree backend in commit 35f83a75529a ("netfilter: nft_set_rbtree: don't gc elements on insert").	2026-03-25	7.8
CVE-2026-23372	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: nfc: rawsock: cancel tx_work before socket teardown In rawsock_release(), cancel any pending tx_work and purge the write queue before orphaning the socket. rawsock_tx_work runs on the system workqueue and calls nfc_data_exchange which dereferences the NCI device. Without synchronization, tx_work can race with socket and device teardown when a process is killed (e.g. by SIGKILL), leading to use-after-free or leaked references. Set SEND_SHUTDOWN first so that if tx_work is already running it will see the flag and skip transmitting, then use cancel_work_sync to wait for any in-progress execution to finish, and finally purge any remaining queued skbs.	2026-03-25	7.8
CVE-2026-23378	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net/sched: act_ife: Fix metalist update behavior Whenever an ife action replace changes the metalist, instead of	2026-03-25	7.8

		replacing the old data on the metalist, the current ife code is appending the new metadata. Aside from being innapropriate behavior, this may lead to an unbounded addition of metadata to the metalist which might cause an out of bounds error when running the encode op: [138.423369][C1] ========== [138.424317][C1] BUG: KASAN: slab-out-of-bounds in ife_tlv_meta_encode (net/ife/ife.c:168) [138.424906][C1] Write of size 4 at addr ffff8880077f4ffe by task ife_out_out_bou/255 [138.425778][C1] CPU: 1 UID: 0 PID: 255 Comm: ife_out_out_bou Not tainted 7.0.0-rc1-00169-gfbdfa8da05b6 #624 PREEMPT(full) [138.425795][C1] Hardware name: Bochs Bochs, BIOS Bochs 01/01/2011 [138.425800][C1] Call Trace: [138.425804][C1] <IRQ> [138.425808][C1] dump_stack_lvl (lib/dump_stack.c:122) [138.425828][C1] print_report (mm/kasan/report.c:379 mm/kasan/report.c:482) [138.425839][C1] ? srso_alias_return_thunk (arch/x86/lib/retpoline.S:221) [138.425844][C1] ? __virt_addr_valid (./arch/x86/include/asm/preempt.h:95 (discriminator 1) ./include/linux/rcupdate.h:975 (discriminator 1) ./include/linux/mmzone.h:2207 (discriminator 1) arch/x86/mm/physaddr.c:54 (discriminator 1)) [138.425853][C1] ? ife_tlv_meta_encode (net/ife/ife.c:168) [138.425859][C1] kasan_report (mm/kasan/report.c:221 mm/kasan/report.c:597) [138.425868][C1] ? ife_tlv_meta_encode (net/ife/ife.c:168) [138.425878][C1] kasan_check_range (mm/kasan/generic.c:186 (discriminator 1) mm/kasan/generic.c:200 (discriminator 1)) [138.425884][C1] __asan_memset (mm/kasan/shadow.c:84 (discriminator 2)) [138.425889][C1] ife_tlv_meta_encode (net/ife/ife.c:168) [138.425893][C1] ? ife_tlv_meta_encode (net/ife/ife.c:171) [138.425898][C1] ? srso_alias_return_thunk (arch/x86/lib/retpoline.S:221) [138.425903][C1] ife_encode_meta_u16 (net/sched/act_ife.c:57) [138.425910][C1] ? __pfx_do_raw_spin_lock (kernel/locking/spinlock_debug.c:114) [138.425916][C1] ? __asan_memcpy (mm/kasan/shadow.c:105 (discriminator 3)) [138.425921][C1] ? __pfx_ife_encode_meta_u16 (net/sched/act_ife.c:45) [138.425927][C1] ? srso_alias_return_thunk (arch/x86/lib/retpoline.S:221) [138.425931][C1] tcf_ife_act (net/sched/act_ife.c:847 net/sched/act_ife.c:879) To solve this issue, fix the replace behavior by adding the metalist to the ife rcu data structure.		
CVE-2026-23383	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: bpf, arm64: Force 8-byte alignment for JIT buffer to prevent atomic tearing struct bpf_plt contains a u64 target field. Currently, the BPF JIT allocator requests an alignment of 4 bytes (sizeof(u32)) for the JIT buffer. Because the base address of the JIT buffer can be 4-byte aligned (e.g., ending in 0x4 or 0xc), the relative padding logic in build_plt() fails to ensure that target lands on an 8-byte boundary. This leads to two issues: 1. UBSAN reports misaligned-access warnings when dereferencing the structure. 2. More critically, target is updated concurrently via WRITE_ONCE() in bpf_arch_text_poke() while the JIT'd code executes ldr. On arm64, 64-bit loads/stores are only guaranteed to be single-copy atomic if they are 64-bit aligned. A misaligned target risks a torn read, causing the JIT to jump to a corrupted address. Fix this by increasing the allocation alignment requirement to 8 bytes (sizeof(u64)) in bpf_jit_binary_pack_alloc(). This anchors the base of the JIT buffer to an 8-byte boundary, allowing the relative padding math in build_plt() to correctly align the target field.	2026-03-25	7.8
CVE-2026-23391	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: netfilter: xt_CT: drop pending enqueued packets on template removal Templates refer to objects that can go away while packets are sitting in nfqueue refer to: - helper, this can be an issue on module removal. - timeout policy, nfnetlink_cttimeout might remove it. The use of templates with zone and event cache filter are safe, since this just copies values. Flush these enqueued packets in case the template rule gets removed.	2026-03-25	7.8
CVE-2026-23392	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: release flowtable after rcu grace period on error	2026-03-25	7.8

		Call synchronize_rcu() after unregistering the hooks from error path, since a hook that already refers to this flowtable can be already registered, exposing this flowtable to packet path and nfnetlink_hook control plane. This error path is rare, it should only happen by reaching the maximum number hooks or by failing to set up to hardware offload, just call synchronize_rcu(). There is a check for already used device hooks by different flowtable that could result in EEXIST at this late stage. The hook parser can be updated to perform this check earlier to this error path really becomes rarely exercised. Uncovered by KASAN reported as use-after-free from nfnetlink_hook path when dumping hooks.		

CVE-2026-23393	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved:
		
		bridge: cfm: Fix race condition in peer_mep deletion
		
		When a peer MEP is being deleted, cancel_delayed_work_sync() is called on ccm_rx_dwork before freeing. However, br_cfm_frame_rx() runs in softirq context under rcu_read_lock (without RTNL) and can re-schedule ccm_rx_dwork via ccm_rx_timer_start() between cancel_delayed_work_sync() returning and kfree_rcu() being called.
		
		The following is a simple race scenario:
		
		cpu0 cpu1
		
		mep_delete_implementation()
		cancel_delayed_work_sync(ccm_rx_dwork);
		br_cfm_frame_rx()
		// peer_mep still in hlist
		if (peer_mep->ccm_defect)
		ccm_rx_timer_start()
		queue_delayed_work(ccm_rx_dwork)
		hlist_del_rcu(&peer_mep->head);
		kfree_rcu(peer_mep, rcu);
		ccm_rx_work_expired()
		// on freed peer_mep
		
		To prevent this, cancel_delayed_work_sync() is replaced with disable_delayed_work_sync() in both peer MEP deletion paths, so that subsequent queue_delayed_work() calls from br_cfm_frame_rx() are silently rejected.
		
		The cc_peer_disable() helper retains cancel_delayed_work_sync() because it is also used for the CC enable/disable toggle path where the work must remain re-schedulable.
			2026-03-25	7.8

CVE-2026-27309	adobe - substance_3d_stager	Substance3D - Stager versions 3.1.7 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.	2026-03-27	7.8
CVE-2026-23920	zabbix - Zabbix	Host and event action script input is validated with a regex (set by the administrator), but the validation runs in multiline mode. If ^ and $ anchors are used in user input validation, an injected newline lets authenticated users bypass the check and inject shell commands.	2026-03-24	7.7
CVE-2026-20125	cisco - multiple products	A vulnerability in the HTTP Server feature of Cisco IOS Software and Cisco IOS XE Software Release 3E could allow an authenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition._x000D_ _x000D_ This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending malformed HTTP requests to an affected device. A successful exploit could allow the attacker to cause a watchdog timer to expire and the device to reload, resulting in a DoS condition. To exploit this vulnerability, the attacker must have a valid user account.	2026-03-25	7.7
CVE-2026-4684	mozilla - multiple products	Race condition, use-after-free in the Graphics: WebRender component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	7.5
CVE-2026-4685	mozilla - multiple products	Incorrect boundary conditions in the Graphics: Canvas2D component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	7.5
CVE-2026-4686	mozilla - multiple products	Incorrect boundary conditions in the Graphics: Canvas2D component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	7.5
CVE-2026-4693	mozilla - multiple products	Incorrect boundary conditions in the Audio/Video: Playback component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	7.5
CVE-2026-4694	mozilla - multiple products	Incorrect boundary conditions, integer overflow in the Graphics component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	7.5

CVE-2026-4695	mozilla - multiple products	Incorrect boundary conditions in the Audio/Video: Web Codecs component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	7.5
CVE-2026-4697	mozilla - multiple products	Incorrect boundary conditions in the Audio/Video: Web Codecs component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	7.5
CVE-2026-4699	mozilla - multiple products	Incorrect boundary conditions in the Layout: Text and Fonts component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	7.5
CVE-2026-4704	mozilla - multiple products	Denial-of-service in the WebRTC: Signaling component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	7.5
CVE-2026-4706	mozilla - multiple products	Incorrect boundary conditions in the Graphics: Canvas2D component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	7.5
CVE-2026-4707	mozilla - multiple products	Incorrect boundary conditions in the Graphics: Canvas2D component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	7.5
CVE-2026-4708	mozilla - multiple products	Incorrect boundary conditions in the Graphics component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	7.5
CVE-2026-4709	mozilla - multiple products	Incorrect boundary conditions in the Audio/Video: GMP component. This vulnerability affects Firefox < 149, Firefox ESR < 115.34, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	7.5
CVE-2026-4712	mozilla - multiple products	Information disclosure in the Widget: Cocoa component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	7.5
CVE-2026-4713	mozilla - multiple products	Incorrect boundary conditions in the Graphics component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	7.5
CVE-2026-4714	mozilla - multiple products	Incorrect boundary conditions in the Audio/Video component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	7.5
CVE-2026-4719	mozilla - multiple products	Incorrect boundary conditions in the Graphics: Text component. This vulnerability affects Firefox < 149, Firefox ESR < 140.9, Thunderbird < 149, and Thunderbird < 140.9.	2026-03-24	7.5
CVE-2026-4726	mozilla - multiple products	Denial-of-service in the XML component. This vulnerability affects Firefox < 149 and Thunderbird < 149.	2026-03-24	7.5
CVE-2026-4727	mozilla - multiple products	Denial-of-service in the Libraries component in NSS. This vulnerability affects Firefox < 149 and Thunderbird < 149.	2026-03-24	7.5
CVE-2026-20622	apple - multiple products	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sequoia 15.7.4, macOS Tahoe 26.3. An app may be able to capture a user's screen.	2026-03-25	7.5
CVE-2026-20639	apple - multiple products	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.3. Processing a maliciously crafted string may lead to heap corruption.	2026-03-25	7.5
CVE-2026-20701	apple - multiple products	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to connect to a network share without user consent.	2026-03-25	7.5
CVE-2026-28837	apple - macos	A logic issue was addressed with improved checks. This issue is fixed in macOS Tahoe 26.4. An app may be able to access sensitive user data.	2026-03-25	7.5
CVE-2026-28842	apple - macos	The issue was addressed with improved bounds checks. This issue is fixed in macOS Tahoe 26.4. A buffer overflow may result in memory corruption and unexpected app termination.	2026-03-25	7.5
CVE-2026-28855	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 26.3 and iPadOS 26.3, macOS Tahoe 26.3. An app may be able to access protected user data.	2026-03-25	7.5
CVE-2026-28865	apple - multiple products	An authentication issue was addressed with improved state management. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. An attacker in a privileged network position may be able to intercept network traffic.	2026-03-25	7.5
CVE-2026-28874	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 26.4 and iPadOS 26.4. A remote attacker may cause an unexpected app termination.	2026-03-25	7.5
CVE-2026-28875	apple - multiple products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 26.4 and iPadOS 26.4. A remote attacker may be able to cause a denial-of-service.	2026-03-25	7.5
CVE-2026-28876	apple - multiple products	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, visionOS 26.4. An app may be able to access sensitive user data.	2026-03-25	7.5
CVE-2026-28894	apple - multiple products	A denial-of-service issue was addressed with improved input validation. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. A remote attacker may be able to cause a denial-of-service.	2026-03-25	7.5
CVE-2026-28377	grafana - tempo	A vulnerability in Grafana Tempo exposes the S3 SSE-C encryption key in plaintext through the /status/config endpoint, potentially allowing unauthorized users to obtain the key used to encrypt trace data stored in S3. Thanks to william_goodfellow for reporting this vulnerability.	2026-03-26	7.5
CVE-2026-27880	grafana - multiple products	The OpenFeature feature toggle evaluation endpoint reads unbounded values into memory, which can cause out-of-memory crashes.	2026-03-27	7.5
CVE-2026-4371	mozilla - multiple products	A malicious mail server could send malformed strings with negative lengths, causing the parser to read memory outside the buffer. If a mail server or connection to a mail server were compromised, an attacker could cause the parser to malfunction, potentially crashing Thunderbird or leaking sensitive data. This vulnerability affects Thunderbird < 149 and Thunderbird < 140.9.	2026-03-24	7.4
CVE-2026-23364	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ksmbd: Compare MACs in constant time To prevent timing attacks, MAC comparisons need to be constant-time. Replace the memcmp() with the correct function, crypto_memneq().	2026-03-25	7.4

CVE-2026-20004	cisco - Cisco IOS XE Software	A vulnerability in the TLS library of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to exhaust the available memory of an affected device._x000D_ _x000D_ This vulnerability is due to improper management of memory resources during TLS connection setup. An attacker could exploit this vulnerability by repeatedly triggering the conditions that cause the memory increase. This could be done in a variety of ways, such as by repeatedly attempting Extensible Authentication Protocol (EAP) authentication when local EAP is enabled on an affected device or by using a machine-in-the-middle attack and resetting TLS connections between the affected device and other devices. A successful exploit could allow the attacker to exhaust the available memory on an affected device, resulting in an unexpected reload and a denial of service (DoS) condition.	2026-03-25	7.4
CVE-2025-15606	tp-link - td-w8961nd_firmware	A Denial-of-Service (DoS) vulnerability in the httpd component of TP-Link's TD-W8961N v4.0 due to improper input sanitization, allows crafted requests to trigger a processing error that causes the httpd service to crash. Successful exploitation may allow the attacker to cause service interruption, resulting in a DoS condition.	2026-03-23	7.1
CVE-2026-23919	zabbix - Zabbix	For performance reasons Zabbix Server/Proxy reuses JavaScript (Duktape) contexts (used in script items, JavaScript reprocessing, Webhooks). This can lead to confidentiality loss where a regular (non-super) Zabbix administrator leaks data for hosts they do not have access to. A fix has been released that makes the built in Zabbix JavaScript objects read-only, but please be advised that usage of global JavaScript variables is not recommended because their content could be leaked. More information in Zabbix documentation.	2026-03-24	7.1
CVE-2026-20687	apple - multiple products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Tahoe 26.4, tvOS 26.4, watchOS 26.4. An app may be able to cause unexpected system termination or write kernel memory.	2026-03-25	7.1
CVE-2025-36258	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 product stores user credentials and other sensitive information in plain text which can be read by a local user.	2026-03-25	7.1
CVE-2026-27663	siemens - multiple products	A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V26.10), RTUM85 RTU Base (All versions < V26.10). The affected application contains denial-of-service (DoS) vulnerability. The remote operation mode is susceptible to a resource exhaustion condition when subjected to a high volume of requests. Sending multiple requests can exhaust resources, preventing parameterization and requiring a reset or reboot to restore functionality.	2026-03-26	7.1
CVE-2026-3622	tp-link - tl-wr841n_firmware	The vulnerability exists in the UPnP component of TL-WR841N v14, where improper input validation leads to an out-of-bounds read, potentially causing a crash of the UPnP service. Successful exploitation can cause the UPnP service to crash, resulting in a Denial-of-Service condition. This vulnerability affects TL-WR841N v14 < EN_0.9.1 4.19 Build 260303 Rel.42399n (V14_260303) and < US_0.9.1.4.19 Build 260312 Rel. 49108n (V14_0304).	2026-03-26	7.1
CVE-2026-23294	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix race in devmap on PREEMPT_RT On PREEMPT_RT kernels, the per-CPU xdp_dev_bulk_queue (bq) can be accessed concurrently by multiple preemptible tasks on the same CPU. The original code assumes bq_enqueue() and __dev_flush() run atomically with respect to each other on the same CPU, relying on local_bh_disable() to prevent preemption. However, on PREEMPT_RT, local_bh_disable() only calls migrate_disable() (when PREEMPT_RT_NEEDS_BH_LOCK is not set) and does not disable preemption, which allows CFS scheduling to preempt a task during bq_xmit_all(), enabling another task on the same CPU to enter bq_enqueue() and operate on the same per-CPU bq concurrently. This leads to several races: 1. Double-free / use-after-free on bq->q[]: bq_xmit_all() snapshots cnt = bq->count, then iterates bq->q[0..cnt-1] to transmit frames. If preempted after the snapshot, a second task can call bq_enqueue() -> bq_xmit_all() on the same bq, transmitting (and freeing) the same frames. When the first task resumes, it operates on stale pointers in bq->q[], causing use-after-free. 2. bq->count and bq->q[] corruption: concurrent bq_enqueue() modifying bq->count and bq->q[] while bq_xmit_all() is reading them. 3. dev_rx/xdp_prog teardown race: __dev_flush() clears bq->dev_rx and bq->xdp_prog after bq_xmit_all(). If preempted between bq_xmit_all() return and bq->dev_rx = NULL, a preempting bq_enqueue() sees dev_rx still set (non-NULL), skips adding bq to the flush_list, and enqueues a frame. When __dev_flush() resumes, it clears dev_rx and removes bq from the flush_list, orphaning the newly enqueued frame. 4. __list_del_clearprev() on flush_node: similar to the cpumap race, both tasks can call __list_del_clearprev() on the same flush_node, the second dereferences the prev pointer already set to NULL.	2026-03-25	7

		The race between task A (__dev_flush -> bq_xmit_all) and task B (bq_enqueue -> bq_xmit_all) on the same CPU: Task A (xdp_do_flush) Task B (ndo_xdp_xmit redirect) ---------- ---------- __dev_flush(flush_list) bq_xmit_all(bq) cnt = bq->count /* e.g. 16 */ /* start iterating bq->q[] */ <-- CFS preempts Task A --> bq_enqueue(dev, xdpf) bq->count == DEV_MAP_BULK_SIZE bq_xmit_all(bq, 0) cnt = bq->count /* same 16! */ ndo_xdp_xmit(bq->q[]) /* frames freed by driver */ bq->count = 0 <-- Task A resumes --> ndo_xdp_xmit(bq->q[]) /* use-after-free: frames already freed! */ Fix this by adding a local_lock_t to xdp_dev_bulk_queue and acquiring it in bq_enqueue() and __dev_flush(). These paths already run under local_bh_disable(), so use local_lock_nested_bh() which on non-RT is a pure annotation with no overhead, and on PREEMPT_RT provides a per-CPU sleeping lock that serializes access to the bq.		
CVE-2026-23923	zabbix - Zabbix	An unauthenticated attacker can exploit the Frontend 'validate' action to blindly instantiate arbitrary PHP classes. The impact depends on environment setup but appears limited at this time.	2026-03-24	6.9
CVE-2025-43534	apple - multiple products	A path handling issue was addressed with improved validation. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.2 and iPadOS 26.2. A user with physical access to an iOS device may be able to bypass Activation Lock.	2026-03-25	6.8
CVE-2025-14917	ibm - websphere_application_server	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.3 IBM WebSphere Application Server Liberty could provide weaker than expected security when administering security settings.	2026-03-25	6.7
CVE-2026-4728	mozilla - multiple products	Spoofing issue in the Privacy: Anti-Tracking component. This vulnerability affects Firefox < 149 and Thunderbird < 149.	2026-03-24	6.5
CVE-2026-3889	mozilla - multiple products	Spoofing issue in Thunderbird. This vulnerability affects Thunderbird < 149 and Thunderbird < 140.9.	2026-03-24	6.5
CVE-2026-20657	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5. Parsing a maliciously crafted file may lead to an unexpected app termination.	2026-03-25	6.5
CVE-2026-20665	apple - multiple products	This issue was addressed through improved state management. This issue is fixed in Safari 26.4, iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. Processing maliciously crafted web content may prevent Content Security Policy from being enforced.	2026-03-25	6.5
CVE-2026-20690	apple - multiple products	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. Processing an audio stream in a maliciously crafted media file may terminate the process.	2026-03-25	6.5
CVE-2026-28835	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. Mounting a maliciously crafted SMB network share may lead to system termination.	2026-03-25	6.5
CVE-2026-28844	apple - macos	A file access issue was addressed with improved input validation. This issue is fixed in macOS Tahoe 26.4. An attacker may gain access to protected parts of the file system.	2026-03-25	6.5
CVE-2026-28857	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.4, iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, visionOS 26.4. Processing maliciously crafted web content may lead to an unexpected process crash.	2026-03-25	6.5
CVE-2026-28863	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 26.4 and iPadOS 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. An app may be able to fingerprint the user.	2026-03-25	6.5
CVE-2026-28878	apple - multiple products	A privacy issue was addressed by removing sensitive data. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sonoma 14.8.5, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. An app may be able to enumerate a user's installed apps.	2026-03-25	6.5
CVE-2026-28879	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. Processing maliciously crafted web content may lead to an unexpected process crash.	2026-03-25	6.5
CVE-2026-28880	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, visionOS 26.4. An app may be able to enumerate a user's installed apps.	2026-03-25	6.5
CVE-2026-20083	cisco - Cisco IOS XE Software	A vulnerability in the Secure Copy Protocol (SCP) server feature of Cisco IOS XE Software could allow an authenticated, local attacker with low privileges to cause a denial of service (DoS) condition on an affected device._x000D_ _x000D_ This vulnerability is due to improper handling of a malformed SCP request. An attacker could exploit this vulnerability by issuing a crafted command through SSH. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition.	2026-03-25	6.5
CVE-2026-20110	cisco - Cisco IOS XE Software	A vulnerability in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device._x000D_ _x000D_ This vulnerability exists because incorrect privileges are associated with the start	2026-03-25	6.5

		maintenance command. An attacker could exploit this vulnerability by accessing the management CLI of the affected device as a low-privileged user and using the start maintenance command. A successful exploit could allow the attacker to put the device in maintenance mode, which shuts down interfaces, resulting in a denial of service (DoS) condition. In case of exploitation, a device administrator can connect to the CLI and use the stop maintenance command to restore operations.		
CVE-2025-14790	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 could allow an attacker to obtain sensitive information due to insufficiently protected credentials.	2026-03-25	6.5
CVE-2025-14807	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 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.	2026-03-25	6.5
CVE-2025-14915	ibm - websphere_application_server	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.3 IBM WebSphere Application Server Liberty is affected by privilege escalation. A privileged user could gain additional access to the application server.	2026-03-25	6.5
CVE-2026-1014	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 is vulnerable to exposure of sensitive information via JSON server response manipulation.	2026-03-25	6.5
CVE-2026-3121	redhat - multiple products	A flaw was found in Keycloak. An administrator with `manage-clients` permission can exploit a misconfiguration where this permission is equivalent to `manage-permissions`. This allows the administrator to escalate privileges and gain control over roles, users, or other administrative functions within the realm. This privilege escalation can occur when admin permissions are enabled at the realm level.	2026-03-26	6.5
CVE-2026-2436	red hat - multiple products	A flaw was found in libsoup's SoupServer. A remote attacker could exploit a use-after-free vulnerability where the `soup_server_disconnect()` function frees connection objects prematurely, even if a TLS handshake is still pending. If the handshake completes after the connection object has been freed, a dangling pointer is accessed, leading to a server crash and a Denial of Service.	2026-03-26	6.5
CVE-2026-0966	red hat - multiple products	The API function `ssh_get_hexa()` is vulnerable, when 0-lenght input is provided to this function. This function is used internally in `ssh_get_fingerprint_hash()` and `ssh_print_hexa()` (deprecated), which is vulnerable to the same input (length is provided by the calling application). The function is also used internally in the gssapi code for logging the OIDs received by the server during GSSAPI authentication. This could be triggered remotely, when the server allows GSSAPI authentication and logging verbosity is set at least to SSH_LOG_PACKET (3). This could cause self-DoS of the per-connection daemon process.	2026-03-26	6.5
CVE-2026-33375	grafana - multiple products	The Grafana MSSQL data source plugin contains a logic flaw that allows a low-privileged user (Viewer) to bypass API restrictions and trigger a catastrophic Out-Of-Memory (OOM) memory exhaustion, crashing the host container.	2026-03-26	6.5
CVE-2026-27877	grafana - multiple products	When using public dashboards and direct data-sources, all direct data-sources' passwords are exposed despite not being used in dashboards. No passwords of proxied data-sources are exposed. We encourage all direct data-sources to be converted to proxied data-sources as far as possible to improve your deployments' security.	2026-03-27	6.5
CVE-2026-27879	grafana - multiple products	A resample query can be used to trigger out-of-memory crashes in Grafana.	2026-03-27	6.5
CVE-2026-28375	grafana - multiple products	A testdata data-source can be used to trigger out-of-memory crashes in Grafana.	2026-03-27	6.5
CVE-2026-28753	f5 - multiple products	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_mail_smtp_module module due to the improper handling of CRLF sequences in DNS responses. This allows an attacker-controlled DNS server to inject arbitrary headers into SMTP upstream requests, leading to potential request manipulation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-03-24	6.3
CVE-2025-14810	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 does not invalidate a session after privileges have been modified which could allow an authenticated user to retain access to sensitive information. CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L CWE: CWE-613: Insufficient Session Expiration CVSS Source: IBM CVSS Base score: 6.3 CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L)	2026-03-25	6.3
CVE-2026-20637	apple - multiple products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.3 and iPadOS 26.3, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.3, tvOS 26.3, visionOS 26.3, watchOS 26.3. An app may be able to cause unexpected system termination.	2026-03-25	6.2
CVE-2026-20651	apple - multiple products	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.4, macOS Tahoe 26.3. An app may be able to access sensitive user data.	2026-03-25	6.2
CVE-2026-20695	apple - multiple products	An information disclosure issue was addressed with improved memory management. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to determine kernel memory layout.	2026-03-25	6.2
CVE-2026-20699	apple - multiple products	A downgrade issue affecting Intel-based Mac computers was addressed with additional code-signing restrictions. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.3, macOS Tahoe 26.4. An app may be able to access user-sensitive data.	2026-03-25	6.2
CVE-2026-28822	apple - multiple products	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. An attacker may be able to cause unexpected app termination.	2026-03-25	6.2

CVE-2026-28833	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, visionOS 26.4. An app may be able to enumerate a user's installed apps.	2026-03-25	6.2
CVE-2026-28841	apple - macos	A buffer overflow was addressed with improved size validation. This issue is fixed in macOS Tahoe 26.4. A buffer overflow may result in memory corruption and unexpected app termination.	2026-03-25	6.2
CVE-2026-28866	apple - multiple products	This issue was addressed with improved validation of symlinks. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access sensitive user data.	2026-03-25	6.2
CVE-2026-28867	apple - multiple products	This issue was addressed with improved authentication. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. An app may be able to leak sensitive kernel state.	2026-03-25	6.2
CVE-2026-28889	apple - xcode	A permissions issue was addressed with additional restrictions. This issue is fixed in Xcode 26.4. An app may be able to read arbitrary files as root.	2026-03-25	6.2
CVE-2025-12708	ibm - concert	IBM Concert 1.0.0 through 2.2.0 contains hard-coded credentials that could be obtained by a local user.	2026-03-25	6.2
CVE-2025-64646	ibm - concert	IBM Concert 1.0.0 through 2.2.0 could allow an attacker to access sensitive information in memory due to the buffer not properly clearing resources.	2026-03-25	6.2
CVE-2026-4647	gnu - multiple products	A flaw was found in the GNU Binutils BFD library, a widely used component for handling binary files such as object files and executables. The issue occurs when processing specially crafted XCOFF object files, where a relocation type value is not properly validated before being used. This can cause the program to read memory outside of intended bounds. As a result, affected tools may crash or expose unintended memory contents, leading to denial-of-service or limited information disclosure risks.	2026-03-23	6.1
CVE-2026-23924	zabbix - Zabbix	Zabbix Agent 2 Docker plugin does not properly sanitize the 'docker.container_info' parameters when forwarding them to the Docker daemon. An attacker capable of invoking Agent 2 can read arbitrary files from running Docker containers by injecting them via the Docker archive API.	2026-03-24	6.1
CVE-2026-20104	cisco - Cisco IOS XE Software	A vulnerability in the bootloader of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches, Cisco Catalyst ESS9300 Embedded Series Switches, Cisco Catalyst IE9310 and IE9320 Rugged Series Switches, and Cisco IE3500 and IE3505 Rugged Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to an affected device to execute arbitrary code at boot time and break the chain of trust._x000D_ _x000D_ This vulnerability is due to insufficient validation of software at boot time. An attacker could exploit this vulnerability by manipulating the loaded binaries on an affected device to bypass some of the integrity checks that are performed during the boot process. A successful exploit could allow the attacker to execute code that bypasses the requirement to run Cisco-signed images._x000D_ _x000D_ Cisco has assigned this security advisory a Security Impact Rating (SIR) of High rather than Medium as the score indicates because this vulnerability allows an attacker to bypass a major security feature of a device.	2026-03-25	6.1
CVE-2026-20115	cisco - Cisco IOS XE Software	A vulnerability in Cisco IOS XE Software for Cisco Meraki could allow a remote, unauthenticated attacker to view confidential device information._x000D_ _x000D_ This vulnerability is due to a device configuration upload being performed over an insecure tunnel. An attacker could exploit this vulnerability by conducting an on-path attack between the affected device and the Cisco Meraki Dashboard. A successful exploit could allow the attacker to view sensitive device configuration information.	2026-03-25	6.1
CVE-2026-4887	red hat - multiple products	A flaw was found in GIMP. This issue is a heap buffer over-read in GIMP PCX file loader due to an off-by-one error. A remote attacker could exploit this by convincing a user to open a specially crafted PCX image. Successful exploitation could lead to out-of-bounds memory disclosure and a possible application crash, resulting in a Denial of Service (DoS).	2026-03-26	6.1
CVE-2026-28297	solarwinds - observability_self-hosted	SolarWinds Observability Self-Hosted was found to be affected by a stored cross-site scripting vulnerability, which when exploited, can lead to unintended script execution.	2026-03-26	6.1
CVE-2026-3260	red hat - multiple products	A flaw was found in Undertow. A remote attacker could exploit this vulnerability by sending an HTTP GET request containing multipart/form-data content. If the underlying application processes parameters using methods like `getParameterMap()`, the server prematurely parses and stores this content to disk. This could lead to resource exhaustion, potentially resulting in a Denial of Service (DoS).	2026-03-24	5.9
CVE-2026-28886	apple - multiple products	A null pointer dereference was addressed with improved input validation. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. A user in a privileged network position may be able to cause a denial-of-service.	2026-03-25	5.9
CVE-2025-64647	ibm - concert	IBM Concert 1.0.0 through 2.2.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information	2026-03-25	5.9
CVE-2025-64648	ibm - concert	IBM Concert 1.0.0 through 2.2.0 transmits data in clear text that could allow an attacker to obtain sensitive information using man in the middle techniques.	2026-03-25	5.9
CVE-2026-28298	solarwinds - observability_self-hosted	SolarWinds Observability Self-Hosted was found to be affected by a stored cross-site scripting vulnerability, which when exploited, can lead to unintended script execution.	2026-03-26	5.9
CVE-2025-14974	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 is vulnerable due to Insecure Direct Object Reference (IDOR).	2026-03-25	5.7
CVE-2026-20633	apple - multiple products	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access user-sensitive data.	2026-03-25	5.5
CVE-2026-20668	apple - multiple products	A logging issue was addressed with improved data redaction. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.3 and iPadOS 26.3, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.3, visionOS 26.3. An app may be able to access sensitive user data.	2026-03-25	5.5
CVE-2026-20670	apple - multiple products	An authorization issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.8.4, macOS Tahoe 26.3. An app may be able to access sensitive user data.	2026-03-25	5.5

CVE-2026-20694	apple - multiple products	This issue was addressed with improved handling of symlinks. This issue is fixed in iOS 26.3 and iPadOS 26.3, macOS Sequoia 15.7.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.4, macOS Sonoma 14.8.5, macOS Tahoe 26.3, macOS Tahoe 26.4. An app may be able to access user-sensitive data.	2026-03-25	5.5
CVE-2026-28825	apple - multiple products	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to modify protected parts of the file system.	2026-03-25	5.5
CVE-2026-28829	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to modify protected parts of the file system.	2026-03-25	5.5
CVE-2026-28831	apple - multiple products	An authorization issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access sensitive user data.	2026-03-25	5.5
CVE-2026-28845	apple - macos	An authorization issue was addressed with improved state management. This issue is fixed in macOS Tahoe 26.4. An app may be able to access protected user data.	2026-03-25	5.5
CVE-2026-28852	apple - multiple products	A stack overflow was addressed with improved input validation. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. An app may be able to cause a denial-of-service.	2026-03-25	5.5
CVE-2026-28868	apple - multiple products	A logging issue was addressed with improved data redaction. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, visionOS 26.4, watchOS 26.4. An app may be able to disclose kernel memory.	2026-03-25	5.5
CVE-2026-28870	apple - multiple products	An information leakage was addressed with additional validation. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. An app may be able to access sensitive user data.	2026-03-25	5.5
CVE-2026-28877	apple - multiple products	An authorization issue was addressed with improved state management. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Tahoe 26.4, visionOS 26.4, watchOS 26.4. An app may be able to access sensitive user data.	2026-03-25	5.5
CVE-2026-28881	apple - macos	A privacy issue was addressed by moving sensitive data. This issue is fixed in macOS Tahoe 26.4. An app may be able to access sensitive user data.	2026-03-25	5.5
CVE-2026-28890	apple - xcode	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 26.4. An app may be able to cause unexpected system termination.	2026-03-25	5.5
CVE-2026-28892	apple - multiple products	A permissions issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to modify protected parts of the file system.	2026-03-25	5.5
CVE-2026-4897	red hat - multiple products	A flaw was found in polkit. A local user can exploit this by providing a specially crafted, excessively long input to the `polkit-agent-helper-1` setuid binary via standard input (stdin). This unbounded input can lead to an out-of-memory (OOM) condition, resulting in a Denial of Service (DoS) for the system.	2026-03-26	5.5
CVE-2026-4948	red hat - multiple products	A flaw was found in firewalld. A local unprivileged user can exploit this vulnerability by mis-authorizing two runtime D-Bus (Desktop Bus) setters, setZoneSettings2 and setPolicySettings. This mis-authorization allows the user to modify the runtime firewall state without proper authentication, leading to unauthorized changes in network security configurations.	2026-03-27	5.5
CVE-2026-20108	cisco - Cisco Catalyst SD-WAN Manager	A vulnerability in the web-based management interface of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device._x000D_ _x000D_ This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of the web-based management interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2026-03-25	5.4
CVE-2026-20114	cisco - Cisco IOS XE Software	A vulnerability in the Lobby Ambassador web-based management API of Cisco IOS XE Software could allow an authenticated, remote attacker to elevate their privileges and access management APIs that would not normally be available for Lobby Ambassador users. _x000D_ _x000D_ This vulnerability exists because parameters that are received by an API endpoint are not sufficiently validated. An attacker could exploit this vulnerability by authenticating as a Lobby Ambassador user and sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to create a new user with privilege level 1 access to the web-based management API. The attacker would then be able to access the device with these new credentials and privileges.	2026-03-25	5.4
CVE-2025-14912	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	2026-03-25	5.4
CVE-2026-1015	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	2026-03-25	5.4
CVE-2026-1561	ibm - websphere_application_server	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.3 IBM WebSphere Application Server Liberty is vulnerable to server-side request forgery (SSRF). This may allow remote attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	2026-03-25	5.4
CVE-2026-2483	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 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	2026-03-25	5.4
CVE-2026-21724	grafana - Grafana OSS	A vulnerability has been discovered in Grafana OSS where an authorization bypass in the provisioning contact points API allows users with Editor role to modify protected webhook URLs without the required alert.notifications.receivers.protected:write permission.	2026-03-26	5.4
CVE-2026-28755	f5 - multiple products	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_stream_ssl_module module due to the improper handling of revoked certificates when configured with the ssl_verify_client on and ssl_ocsp on directives, allowing the TLS handshake to succeed even after an OCSP check identifies the certificate as revoked.	2026-03-24	5.3

		Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
CVE-2026-20632	apple - macos	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Tahoe 26.4. An app may be able to access sensitive user data.	2026-03-25	5.3
CVE-2026-20686	apple - multiple products	This issue was addressed with improved input validation. This issue is fixed in iOS 26.3 and iPadOS 26.3. An app may be able to access sensitive user data.	2026-03-25	5.3
CVE-2026-20692	apple - multiple products	A privacy issue was addressed with improved handling of user preferences. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. "Hide IP Address" and "Block All Remote Content" may not apply to all mail content.	2026-03-25	5.3
CVE-2026-20697	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access sensitive user data.	2026-03-25	5.3
CVE-2026-28818	apple - multiple products	A logging issue was addressed with improved data redaction. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access sensitive user data.	2026-03-25	5.3
CVE-2026-28820	apple - macos	This issue was addressed with improved checks. This issue is fixed in macOS Tahoe 26.4. An app may be able to access sensitive user data.	2026-03-25	5.3
CVE-2026-28824	apple - multiple products	An authorization issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access sensitive user data.	2026-03-25	5.3
CVE-2026-28828	apple - multiple products	A permissions issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access sensitive user data.	2026-03-25	5.3
CVE-2026-28838	apple - multiple products	A permissions issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to break out of its sandbox.	2026-03-25	5.3
CVE-2026-28839	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access sensitive user data.	2026-03-25	5.3
CVE-2026-28862	apple - multiple products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access user-sensitive data.	2026-03-25	5.3
CVE-2026-20113	cisco - Cisco IOS XE Software	A vulnerability in the web-based Cisco IOx application hosting environment management interface of Cisco IOS XE Software could allow an unauthenticated, remote attacker to perform a carriage return line feed (CRLF) injection attack against a user._x000D_ _x000D_ This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by sending crafted packets to an affected device. A successful exploit could allow the attacker to arbitrarily inject log entries, manipulate the structure of log files, or obscure legitimate log events.	2026-03-25	5.3
CVE-2026-2100	red hat - multiple products	A flaw was found in p11-kit. A remote attacker could exploit this vulnerability by calling the C_DeriveKey function on a remote token with specific IBM kyber or IBM btc derive mechanism parameters set to NULL. This could lead to the RPC-client attempting to return an uninitialized value, potentially resulting in a NULL dereference or undefined behavior. This issue may cause an application level denial of service or other unpredictable system states.	2026-03-26	5.3
CVE-2026-1940	red hat - multiple products	An incomplete fix for CVE-2024-47778 allows an out-of-bounds read in gst_wavparse_adtl_chunk() function. The patch added a size validation check lsize + 8 > size, but it does not account for the GST_ROUND_UP_2(lsize) used in the actual offset calculation. When lsize is an odd number, the parser advances more bytes than validated, causing OOB read.	2026-03-23	5.1
CVE-2026-28834	apple - multiple products	A race condition was addressed with improved state handling. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to cause unexpected system termination.	2026-03-25	5.1
CVE-2026-28888	apple - multiple products	A race condition was addressed with improved state handling. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to gain root privileges.	2026-03-25	5.1
CVE-2025-36438	ibm - concert	IBM Concert 1.0.0 through 2.2.0 could allow a privileged user to perform unauthorized actions due to improper restriction of channel communication to intended endpoints.	2026-03-25	5.1
CVE-2025-36440	ibm - concert	IBM Concert 1.0.0 through 2.2.0 could allow a local user to obtain sensitive information due to missing function level access control.	2026-03-25	5.1
CVE-2026-4346	tp-link - tl-wr850n_firmware	The vulnerability affecting TL-WR850N v3 allows cleartext storage of administrative and Wi-Fi credentials in a region of the device's flash memory while the serial interface remains enabled and protected by weak authentication. An attacker with physical access and the ability to connect to the serial port can recover sensitive information, including the router's management password and wireless network key. Successful exploitation can lead to full administrative control of the device and unauthorized access to the associated wireless network.	2026-03-26	5.1
CVE-2026-0964	red hat - multiple products	A malicious SCP server can send unexpected paths that could make the client application override local files outside of working directory. This could be misused to create malicious executable or configuration files and make the user execute them under specific consequences. This is the same issue as in OpenSSH, tracked as CVE-2019-6111.	2026-03-26	5
CVE-2026-20693	apple - multiple products	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An attacker with root privileges may be able to delete protected system files.	2026-03-25	4.9
CVE-2026-28823	apple - macos	A path handling issue was addressed with improved validation. This issue is fixed in macOS Tahoe 26.4. An app with root privileges may be able to delete protected system files.	2026-03-25	4.9
CVE-2026-20112	cisco - Cisco IOS XE Software	A vulnerability in the web-based Cisco IOx application hosting environment management interface of Cisco IOS XE Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device._x000D_ _x000D_ This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful	2026-03-25	4.8

		exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have valid administrative credentials.		
CVE-2026-2485	ibm - infosphere_information_server	IBM Infosphere Information Server 11.7.0.0 through 11.7.1.6 is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2026-03-25	4.8
CVE-2026-28856	apple - multiple products	The issue was addressed with improved authentication. This issue is fixed in iOS 26.4 and iPadOS 26.4, visionOS 26.4, watchOS 26.4. An attacker with physical access to a locked device may be able to view sensitive user information.	2026-03-25	4.6
CVE-2026-28895	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 26.4 and iPadOS 26.4. An attacker with physical access to an iOS device with Stolen Device Protection enabled may be able to access biometrics-gated Protected Apps with the passcode.	2026-03-25	4.6
CVE-2025-36187	ibm - multiple products	IBM Knowledge Catalog Standard Cartridge 5.0.0, 5.0.1, 5.0.2, 5.0.3, 5.1, 5.1.1, 5,1.2, 5.1.3, 5.2.0, 5.2.1 stores potentially sensitive information in log files that could be read by a local privileged user.	2026-03-25	4.4
CVE-2026-4628	redhat - build_of_keycloak	A flaw was found in Keycloak. An improper Access Control vulnerability in Keycloak's User-Managed Access (UMA) resource_set endpoint allows attackers with valid credentials to bypass the allowRemoteResourceManagement=false restriction. This occurs due to incomplete enforcement of access control checks on PUT operations to the resource_set endpoint. This issue enables unauthorized modification of protected resources, impacting data integrity.	2026-03-23	4.3
CVE-2026-20664	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.4, iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, visionOS 26.4. Processing maliciously crafted web content may lead to an unexpected process crash.	2026-03-25	4.3
CVE-2026-20691	apple - multiple products	An authorization issue was addressed with improved state management. This issue is fixed in Safari 26.4, iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, visionOS 26.4, watchOS 26.4. A maliciously crafted webpage may be able to fingerprint the user.	2026-03-25	4.3
CVE-2026-28859	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.4, iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. A malicious website may be able to process restricted web content outside the sandbox.	2026-03-25	4.3
CVE-2026-28861	apple - multiple products	A logic issue was addressed with improved state management. This issue is fixed in Safari 26.4, iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, visionOS 26.4. A malicious website may be able to access script message handlers intended for other origins.	2026-03-25	4.3
CVE-2026-28871	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in Safari 26.4, iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4. Visiting a maliciously crafted website may lead to a cross-site scripting attack.	2026-03-25	4.3
CVE-2025-36422	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 IBM InfoSphere DataStage Flow Designer 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.	2026-03-25	4.3
CVE-2026-1262	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 is affected by an information disclosure vulnerability.	2026-03-25	4.3
CVE-2026-2484	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 is affected by an information exposure vulnerability caused by overly verbose error messages	2026-03-25	4.3
CVE-2026-3190	redhat - build_of_keycloak	A flaw was found in Keycloak. The User-Managed Access (UMA) 2.0 Protection API endpoint for permission tickets fails to enforce the `uma_protection` role check. This allows any authenticated user with a token issued for a resource server client, even without the `uma_protection` role, to enumerate all permission tickets in the system. This vulnerability partial leads to information disclosure.	2026-03-26	4.3
CVE-2026-32187	microsoft - edge	Microsoft Edge (Chromium-based) Defense in Depth Vulnerability	2026-03-27	4.2
CVE-2026-20607	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to access protected user data.	2026-03-25	4
CVE-2026-28816	apple - multiple products	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4. An app may be able to delete files for which it does not have permission.	2026-03-25	4
CVE-2026-28826	apple - macos	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Tahoe 26.4. A malicious app may be able to break out of its sandbox.	2026-03-25	4
CVE-2026-28882	apple - multiple products	This issue was addressed with improved checks. This issue is fixed in iOS 26.4 and iPadOS 26.4, macOS Tahoe 26.4, tvOS 26.4, visionOS 26.4, watchOS 26.4. An app may be able to enumerate a user's installed apps.	2026-03-25	4
CVE-2025-14684	ibm - multiple products	IBM Maximo Application Suite - Monitor Component 9.1, 9.0, 8.11, and 8.10 could allow an unauthorized user to inject data into log messages due to improper neutralization of special elements when written to log files.	2026-03-25	4
CVE-2026-4633	redhat - build_of_keycloak	A flaw was found in Keycloak. A remote attacker can exploit differential error messages during the identity-first login flow when Organizations are enabled. This vulnerability allows an attacker to determine the existence of users, leading to information disclosure through user enumeration.	2026-03-23	3.7
CVE-2026-20684	apple - macos	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Tahoe 26.4. An app may bypass Gatekeeper checks.	2026-03-25	3.3
CVE-2026-28864	apple - multiple products	This issue was addressed with improved permissions checking. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4, visionOS 26.4, watchOS 26.4. A local attacker may gain access to user's Keychain items.	2026-03-25	3.3
CVE-2026-28893	apple - macos	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Tahoe 26.4. A document may be written to a temporary file when using print preview.	2026-03-25	3.3
CVE-2026-2271	red hat - multiple products	A flaw was found in GIMP's PSP (Paint Shop Pro) file parser. A remote attacker could exploit an integer overflow vulnerability in the read_creator_block() function by providing a specially crafted PSP image file. This vulnerability occurs when a 32-bit length value from the file is used for memory allocation without proper validation, leading to a heap overflow and an out-of-bounds write. Successful exploitation could result in an application level denial of service.	2026-03-26	3.3

CVE-2025-14808	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 could allow an attacker to obtain sensitive information from the query string of an HTTP GET method to process a request which could be obtained using man in the middle techniques.	2026-03-25	3.1
CVE-2026-4874	redhat - multiple products	A flaw was found in Keycloak. An authenticated attacker can perform Server-Side Request Forgery (SSRF) by manipulating the `client_session_host` parameter during refresh token requests. This occurs when a Keycloak client is configured to use the `backchannel.logout.url` with the `application.session.host` placeholder. Successful exploitation allows the attacker to make HTTP requests from the Keycloak server's network context, potentially probing internal networks or internal APIs, leading to information disclosure.	2026-03-26	3.1
CVE-2026-32642	apache - multiple products	Incorrect Authorization (CWE-863) vulnerability in Apache Artemis, Apache ActiveMQ Artemis exists when an application using the OpenWire protocol attempts to create a non-durable JMS topic subscription on an address that doesn't exist with an authenticated user which has the "createDurableQueue" permission but does not have the "createAddress" permission and address auto-creation is disabled. In this circumstance, a temporary address will be created whereas the attempt to create the non-durable subscription should instead fail since the user is not authorized to create the corresponding address. When the OpenWire connection is closed the address is removed. This issue affects Apache Artemis: from 2.50.0 through 2.52.0; Apache ActiveMQ Artemis: from 2.0.0 through 2.44.0. Users are recommended to upgrade to version 2.53.0, which fixes the issue.	2026-03-24	2.3
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.