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 17 مايو إلى 23 مايو. 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 17th of May to 23rd of May. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2026-42822	microsoft - multiple products	Improper authentication in Azure Local Disconnected Operations allows an unauthorized attacker to elevate privileges over a network.	2026-05-18	10
CVE-2026-20223	cisco - Cisco Secure Workload	A vulnerability in the access validation of internal REST APIs of Cisco Secure Workload could allow an unauthenticated, remote attacker to access site resources with the privileges of the Site Admin role. This vulnerability is due to insufficient validation and authentication when accessing REST API endpoints. An attacker could exploit this vulnerability if they are able to send a crafted API request to an affected endpoint. A successful exploit could allow the attacker to read sensitive information and make configuration changes across tenant boundaries with the privileges of the Site Admin user.	2026-05-20	10
CVE-2026-23652	microsoft - power_pages	Improper neutralization of special elements used in a command ('command injection') in Microsoft Power Pages allows an unauthorized attacker to execute code over a network.	2026-05-22	10
CVE-2026-40412	microsoft - azure_orbital_spatio	Unrestricted upload of file with dangerous type in Azure Orbital Spatio allows an unauthorized attacker to execute code over a network.	2026-05-22	10
CVE-2026-41104	microsoft - planetary_computer	Deserialization of untrusted data in Microsoft Planetary Computer Pro allows an unauthorized attacker to disclose information over a network.	2026-05-22	10
CVE-2026-42901	microsoft - entra_id	Origin validation error in Microsoft Entra ID allows an unauthorized attacker to elevate privileges over a network.	2026-05-22	10
CVE-2026-47280	microsoft - azure_resource_manager	Improper authentication in Azure Resource Manager (ARM) allows an unauthorized attacker to elevate privileges over a network.	2026-05-22	10
CVE-2026-40411	microsoft - azure_virtual_network_gateway	Improper input validation in Azure Virtual Network Gateway allows an authorized attacker to execute code over a network.	2026-05-22	9.9
CVE-2026-45434	apache - ofbiz	Improper Authentication vulnerability in Apache OFBiz via Password-Change Logic Flaw Leading to Remote Code Execution This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	2026-05-19	9.8
CVE-2026-43493	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: crypto: pcrypt - Fix handling of MAY_BACKLOG requests MAY_BACKLOG requests can return EBUSY. Handle them by checking for that value and filtering out EINPROGRESS notifications.	2026-05-19	9.8
CVE-2026-47323	apache software foundation - Apache Camel	Camel-CXF and Camel-Knative Message Header Injection via Missing Inbound Filtering The CXF and Knative HeaderFilterStrategy implementations (CxfRsHeaderFilterStrategy in camel-cxf-rest, CxfHeaderFilterStrategy in camel-cxf-transport, and KnativeHttpHeaderFilterStrategy in camel-knative-http) only filter outbound Camel-internal headers via setOutFilterStartsWith, while not configuring inbound filtering via setInFilterStartsWith. As a result, an unauthenticated attacker can inject Camel-internal headers (e.g. CamelExecCommandExecutable, CamelFileName) via HTTP requests to CXF-RS or CXF-SOAP endpoints. When a route forwards messages from these endpoints to header-driven components such as camel-exec or camel-file, the injected headers override configured values, enabling remote code execution or arbitrary file writes. This is the same pattern that was previously addressed in camel-undertow (CVE-2025-30177), the broader incoming-header filter (CVE-2025-27636 and CVE-2025-29891), and non-HTTP strategies (CVE-2026-40453). This issue affects Apache Camel: from 3.18.0 before 4.14.6, from 4.15.0 before 4.18.2. Users are	2026-05-19	9.8

		recommended to upgrade to version 4.19.0, which fixes the issue. If users are on the 4.18.x LTS releases stream, then they are suggested to upgrade to 4.18.2. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.6.		
CVE-2026-8956	mozilla - multiple products	Integer overflow in the Networking: JAR component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	2026-05-19	9.8
CVE-2026-9082	drupal - multiple products	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Drupal Drupal core allows SQL Injection. This issue affects Drupal core: from 8.9.0 before 10.4.10, from 10.5.0 before 10.5.10, from 10.6.0 before 10.6.9, from 11.0.0 before 11.1.10, from 11.2.0 before 11.2.12, from 11.3.0 before 11.3.10.	2026-05-20	9.8
CVE-2026-43501	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ipv6: rpl: reserve mac_len headroom when recompressed SRH grows ipv6_rpl_srh_rcv() decompresses an RFC 6554 Source Routing Header, swaps the next segment into ipv6_hdr->daddr, recompresses, then pulls the old header and pushes the new one plus the IPv6 header back. The recompressed header can be larger than the received one when the swap reduces the common-prefix length the segments share with daddr (CmprI=0,CmprE>0, seg[0][0] != daddr[0] gives the maximum +8 bytes). pskb_expand_head() was gated on segments_left == 0, so on earlier segments the push consumed unchecked headroom. Once skb_push() leaves fewer than skb->mac_len bytes in front of data, skb_mac_header_rebuild()'s call to: skb_set_mac_header(skb, -skb->mac_len); will store (data - head) - mac_len into the u16 mac_header field, which wraps to ~65530, and the following memmove() writes mac_len bytes ~64KiB past skb->head. A single AF_INET6/SOCK_RAW/IPV6_HDRINCL packet over lo with a two segment type-3 SRH (CmprI=0, CmprE=15) reaches headroom 8 after one pass; KASAN reports a 14-byte OOB write in ipv6_rthdr_rcv. Fix this by expanding the head whenever the remaining room is less than the push size plus mac_len, and request that much extra so the rebuilt MAC header fits afterwards.	2026-05-21	9.8
CVE-2025-71210	trendmicro - multiple products	A vulnerability in the Trend Micro Apex One management console could allow a remote attacker to upload malicious code and execute commands on affected installations. Please note: although this vulnerability carries a technical critical CVSS rating, this was reported via responsible disclosure via a researcher through the Zero Day Initiative. The SaaS versions of the product have already been mitigated and no customer action required. For this particular vulnerability, an attacker must have access to the Trend Micro Apex One Management Console, so customers that have their console's IP address exposed externally should consider mitigating factors such as source restrictions if not already applied.	2026-05-21	9.8
CVE-2025-71211	trendmicro - multiple products	A vulnerability in the Trend Micro Apex One management console could allow a remote attacker to upload malicious code and execute commands on affected installations. This vulnerability is similar in scope to CVE-2025-71210 but affects a different executable. Please note: although this vulnerability carries a technical critical CVSS rating, this was reported via responsible disclosure via a researcher through the Zero Day Initiative. The SaaS versions of the product have already been mitigated and no customer action required. For this particular vulnerability, an attacker must have access to the Trend Micro Apex One Management Console, so customers that have their console's IP address exposed externally should consider mitigating factors such as source restrictions if not already applied.	2026-05-21	9.8
CVE-2026-48207	apache - fory	Deserialization of untrusted data in Apache Fory PyFory. PyFory's ReduceSerializer could bypass documented DeserializationPolicy validation hooks during reduce-state restoration and global-name resolution. An application is vulnerable if it deserializes attacker-controlled data using PyFory Python-native mode with strict mode disabled and relies on DeserializationPolicy to restrict unsafe classes, functions, or module attributes. This issue affects Apache Fory: from before 1.0.0. Mitigation: Users of Apache Fory are recommended to upgrade to version 1.0.0 or later, which enforces DeserializationPolicy validation for the affected ReduceSerializer paths and thus fixes this issue.	2026-05-21	9.8
CVE-2026-44930	apache - multiple products	An LDAP injection vulnerability in the LDAP Certificate repository of the XKMS server in Apache CXF may allow an attacker to retrieve arbitrary certificates from the repository. Users are recommended to upgrade to versions 4.2.1, 4.1.6 or 3.6.11, which fix this issue.	2026-05-22	9.8
CVE-2026-8953	mozilla - multiple products	Sandbox escape due to use-after-free in the Disability Access APIs component. This vulnerability was fixed in Firefox 151, Firefox ESR 115.36, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	2026-05-19	9.6
CVE-2026-8959	mozilla - multiple products	Sandbox escape due to incorrect boundary conditions in the Widget: Win32 component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	2026-05-19	9.6
CVE-2026-8950	mozilla - multiple products	Same-origin policy bypass in the Networking: HTTP component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	2026-05-19	9.3
CVE-2026-8631	hp - linux_imaging_and_printing	A potential security vulnerability has been identified in the HP Linux Imaging and Printing Software. This potential vulnerability may allow escalation of privileges and/or arbitrary code execution via an integer overflow in the hpcups processing path when handling crafted print data.	2026-05-20	9.3
CVE-2026-41090	microsoft - 365_copilot	Improper neutralization of special elements used in a command ('command injection') in Microsoft Copilot allows an unauthorized attacker to perform tampering over a network.	2026-05-22	9.3

CVE-2026-8711	f5 - NGINX JavaScript	NGINX JavaScript has a vulnerability when the js_fetch_proxy directive is configured with at least one client-controlled NGINX variable (for example, $http_*, $arg_*, $cookie_*) and a location invoking the ngx.fetch() operation from NGINX JavaScript. An unauthenticated attacker can exploit this vulnerability by sending crafted HTTP requests. This may cause a heap buffer overflow in the NGINX worker process leading to a restart. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-19	9.2
CVE-2026-9256	f5 - multiple products	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_rewrite_module module. This vulnerability exists when a rewrite directive uses a regex pattern with distinct, overlapping Perl-Compatible Regular Expression (PCRE) captures (for example, ^/((.*))$) and a replacement string that references multiple such captures (for example, $1$2) in a redirect or arguments context. An unauthenticated attacker along with conditions beyond their control can exploit this vulnerability by sending crafted HTTP requests. This may cause a heap buffer overflow in the NGINX worker process leading to a restart. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-22	9.2
CVE-2026-31986	apache - ofbiz	Use of Hard-coded Cryptographic Key vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	2026-05-19	9.1
CVE-2026-41919	apache - ofbiz	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	2026-05-19	9.1
CVE-2026-8948	mozilla - multiple products	Same-origin policy bypass in the DOM: Networking component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	2026-05-19	9.1
CVE-2026-33843	microsoft - entra_id	Authentication bypass using an alternate path or channel in Microsoft Azure Active Directory B2C allows an unauthorized attacker to elevate privileges over a network.	2026-05-22	9.1
CVE-2026-45495	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2026-05-18	8.8
CVE-2026-46586	apache - ofbiz	Improper Control of Generation of Code ('Code Injection'), Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	2026-05-19	8.8
CVE-2026-8952	mozilla - multiple products	Privilege escalation in the Application Update component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	2026-05-19	8.8
CVE-2026-8955	mozilla - multiple products	Privilege escalation in the DOM: Workers component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	2026-05-19	8.8
CVE-2026-8957	mozilla - multiple products	Privilege escalation in the Enterprise Policies component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	2026-05-19	8.8
CVE-2026-8970	mozilla - multiple products	Privilege escalation in the Security component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	2026-05-19	8.8
CVE-2026-8972	mozilla - multiple products	Privilege escalation in the WebRTC: Audio/Video component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	2026-05-19	8.8
CVE-2026-8973	mozilla - multiple products	Memory safety bugs present in Firefox 150. 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 was fixed in Firefox 151 and Thunderbird 151.	2026-05-19	8.8
CVE-2026-8974	mozilla - multiple products	Memory safety bugs present in Firefox ESR 140.10 and Firefox 150. 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 was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	2026-05-19	8.8
CVE-2026-8975	mozilla - multiple products	Memory safety bugs present in Firefox ESR 115.35, Firefox ESR 140.10 and Firefox 150. 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 was fixed in Firefox 151, Firefox ESR 115.36, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	2026-05-19	8.8
CVE-2026-44925	veritas - infoscale_operations_manager	Cross-Site Request Forgery (CSRF) vulnerability in InfoScale v.9.1.3 Operations Manager (VIOM) allows an attacker to force the user with an active session into clicking a malicious HTML link, which triggers unintended modifications on VIOM web application without the user's knowledge.	2026-05-20	8.8
CVE-2026-9111	google - chrome	Use after free in WebRTC in Google Chrome on Linux prior to 148.0.7778.179 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	2026-05-20	8.8
CVE-2026-9112	google - chrome	Use after free in GPU in Google Chrome on Windows prior to 148.0.7778.179 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-05-20	8.8
CVE-2026-9114	google - chrome	Use after free in QUIC in Google Chrome on prior to 148.0.7778.179 allowed a remote attacker to execute arbitrary code inside a sandbox via malicious network traffic. (Chromium security severity: High)	2026-05-20	8.8
CVE-2026-9118	google - chrome	Use after free in XR in Google Chrome on Windows prior to 148.0.7778.179 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	2026-05-20	8.8

CVE-2026-9119	google - chrome	Heap buffer overflow in WebRTC in Google Chrome on prior to 148.0.7778.179 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-05-20	8.8
CVE-2026-9120	google - chrome	Use after free in WebRTC in Google Chrome prior to 148.0.7778.179 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	2026-05-20	8.8
CVE-2026-9121	google - chrome	Out of bounds read in GPU in Google Chrome on prior to 148.0.7778.179 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2026-05-20	8.8
CVE-2026-9126	google - chrome	Use after free in DOM in Google Chrome on prior to 148.0.7778.179 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-05-20	8.8
CVE-2026-43495	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net: wwan: t7xx: validate port_count against message length in t7xx_port_enum_msg_handler t7xx_port_enum_msg_handler() uses the modem-supplied port_count field as a loop bound over port_msg->data[] without checking that the message buffer contains sufficient data. A modem sending port_count=65535 in a 12-byte buffer triggers a slab-out-of-bounds read of up to 262140 bytes. Add a sizeof(*port_msg) check before accessing the port message header fields to guard against undersized messages. Add a struct_size() check after extracting port_count and before the loop. In t7xx_parse_host_rt_data(), guard the rt_feature header read with a remaining-buffer check before accessing data_len, validate feat_data_len against the actual remaining buffer to prevent OOB reads and signed integer overflow on offset. Pass msg_len from both call sites: skb->len at the DPMAIF path after skb_pull(), and the validated feat_data_len at the handshake path.	2026-05-21	8.8
CVE-2026-8992	ivanti - multiple products	An improper certificate validation vulnerability in Ivanti Secure Access Client before 22.8R6 allows a remote unauthenticated attacker to execute arbitrary code.	2026-05-22	8.8
CVE-2026-6406	docker - docker_desktop	The Docker CLI --use-api-socket flag bypasses Enhanced Container Isolation (ECI) restrictions in Docker Desktop. When ECI is enabled, Docker socket mounts from containers are denied unless explicitly allowed via the admin-settings configuration. However, the --use-api-socket flag adds the Docker socket mount via the HostConfig.Mounts field rather than the HostConfig.Binds field. The ECI enforcement in the Docker Desktop API proxy only inspected Binds, allowing the mount to pass unchecked. This grants a container full access to the Docker Engine socket and, if the host user has logged in to container registries, their authentication credentials. A local attacker with the ability to run Docker CLI commands can exploit this to escape ECI restrictions, access the Docker Engine, and potentially escalate privileges.	2026-05-22	8.8
CVE-2026-5817	docker - Docker Desktop	The vllm-metal inference backend in Docker Model Runner on macOS unconditionally sets trust_remote_code=True when loading model tokenizers, and runs without sandboxing. This causes transformers.AutoTokenizer.from_pretrained() to import and execute arbitrary Python files included in any model pulled from an OCI registry, resulting in arbitrary code execution on the Docker host as the Docker Desktop user when inference is triggered. Any container on the Docker network can trigger this by calling the model-runner.docker.internal API to pull a malicious model and request inference.	2026-05-22	8.8
CVE-2026-5843	docker - Docker Desktop	The MLX inference backend in Docker Model Runner on macOS uses the MLX-LM library, which unconditionally imports and executes arbitrary Python files from model directories via the model_file configuration field in config.json. When a model's config.json specifies a model_file pointing to a Python file, MLX-LM uses importlib to load and execute it with no trust_remote_code gate or equivalent safety check. The MLX backend runs without sandboxing, resulting in arbitrary code execution on the Docker host as the Docker Desktop user. Any container on the Docker network can trigger this by calling the model-runner.docker.internal API to pull a malicious model from an attacker-controlled OCI registry and request inference.	2026-05-22	8.8
CVE-2026-35430	microsoft - azure_privileged_identity_management	Authorization bypass through user-controlled key in Azure Privileged Identity Management (PIM) allows an authorized attacker to elevate privileges over a network.	2026-05-22	8.8
CVE-2026-45659	microsoft - multiple products	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-05-22	8.8
CVE-2026-43503	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net: skbuff: propagate shared-frag marker through frag-transfer helpers Two frag-transfer helpers (__pskb_copy_fclone() and skb_shift()) fail to propagate the SKBFL_SHARED_FRAG bit in skb_shinfo()->flags when moving frags from source to destination. __pskb_copy_fclone() defers the rest of the shinfo metadata to skb_copy_header() after copying frag descriptors, but that helper only carries over gso_{size,segs,type} and never touches skb_shinfo()->flags; skb_shift() moves frag descriptors directly and leaves flags untouched. As a result, the destination skb keeps a reference to the same externally-owned or page-cache-backed pages while reporting skb_has_shared_frag() as false.	2026-05-23	8.8

		The mismatch is harmful in any in-place writer that uses skb_has_shared_frag() to decide whether shared pages must be detoured through skb_cow_data(). ESP input is one such writer (esp4.c, esp6.c), and a single nft 'dup to <local>' rule -- or any other nf_dup_ipv4() / xt_TEE caller -- is enough to land a pskb_copy()'d skb in esp_input() with the marker stripped, letting an unprivileged user write into the page cache of a root-owned read-only file via authencesn-ESN stray writes. Set SKBFL_SHARED_FRAG on the destination whenever frag descriptors were actually moved from the source. skb_copy() and skb_copy_expand() share skb_copy_header() too but linearize all paged data into freshly allocated head storage and emerge with nr_frags == 0, so skb_has_shared_frag() returns false on its own; they need no change. The same omission exists in skb_gro_receive() and skb_gro_receive_list(). The former moves the incoming skb's frag descriptors into the accumulator's last sub-skb via two paths (a direct frag-move loop and the head_frag + memcpy path); the latter chains the incoming skb whole onto p's frag_list. Downstream skb_segment() reads only skb_shinfo(p)->flags, and skb_segment_list() reuses each sub-skb's shinfo as the nskb -- both p and lp must carry the marker. The same omission also exists in tcp_clone_payload(), which builds an MTU probe skb by moving frag descriptors from skbs on sk_write_queue into a freshly allocated nskb. The helper falls into the same family and warrants the same fix for consistency; no TCP TX-side in-place writer is currently known to reach a user page through this gap, but a future consumer depending on the marker would regress silently. The same omission exists in skb_segment(): the per-iteration flag merge takes only head_skb's flag, and the inner switch that rebinds frag_skb to list_skb on head_skb-frags exhaustion does not fold the new frag_skb's flag into nskb. Fold frag_skb's flag at both sites so segments drawing frags from frag_list members carry the marker.		
CVE-2026-27173	apache software foundation - Apache Airflow CNCF Kubernetes provider	JWT tokens that were used by workers in Kubernetes Executors have been exposed to users who had read only access to Kuberentes Pods. This could allow users with just read-only access to perform actions that were only available to running tasks via Task SDK and potentially allow to modify state of Airflow Database for tasks.	2026-05-19	8.7
CVE-2018-25358	d-link - DIR-601	D-Link DIR601 2.02NA contains a credential disclosure vulnerability that allows unauthenticated attackers to retrieve sensitive configuration data by manipulating the table_name parameter in POST requests. Attackers can send requests to /my_cgi.cgi with table_name values like admin_user, wireless_settings, and wireless_security to extract administrative credentials and wireless network keys in clear text.	2026-05-23	8.7
CVE-2026-8958	mozilla - multiple products	Information disclosure, sandbox escape in the Security: Process Sandboxing component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	2026-05-19	8.6
CVE-2026-8632	hp - linux_imaging_and_printing	A potential security vulnerability has been identified in the HP Linux Imaging and Printing Software. This potential vulnerability may allow escalation of privileges and/or arbitrary code execution via operating system command injection.	2026-05-20	8.5
CVE-2026-2740	zohocorp - multiple products	Zohocorp ManageEngine ADSelfService Plus version before 6525, DataSecurity Plus before 6264 and RecoveryManager Plus before 6313 are vulnerable to Authenticated Remote code execution in the agent machines due to the bug in the 3rd party dependency.	2026-05-21	8.4
CVE-2026-7504	red hat - multiple products	A flaw was found in Keycloak's URL validation logic during redirect operations. By crafting a malicious request, an attacker could bypass validation to redirect users to unauthorized URLs, potentially leading to the exposure of sensitive information within the domain or facilitating further attacks. This vulnerability specifically affects Keycloak clients configured with a wildcard (*) in the "Valid Redirect URIs" field and requires user interaction to be successfully exploited. The issue stems from a discrepancy in how Keycloak and the underlying Java URI implementation handle the user-info component of a URL. If a malicious redirect URL is constructed using multiple @ characters in the user-info section, Java's URI parser fails to extract the user-info, leaving only the raw authority field. Consequently, Keycloak's validation check fails to detect the malformed user-info, falls back to a wildcard comparison, and incorrectly permits the malicious redirect.	2026-05-19	8.1
CVE-2026-8962	mozilla - multiple products	Mitigation bypass in the DOM: Security component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	2026-05-19	8.1
CVE-2026-8969	mozilla - multiple products	Mitigation bypass in the DOM: Security component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	2026-05-19	8.1
CVE-2026-45584	microsoft - malware_protection_engine	Heap-based buffer overflow in Microsoft Defender allows an unauthorized attacker to execute code over a network.	2026-05-20	8.1
CVE-2026-45760	apache software foundation - Apache Camel K	(Externally Controlled Reference to a Resource in Another Sphere), (Authorization Bypass Through User-Controlled Key) vulnerability in Apache Camel K. Authorized users in a Kubernetes namespace can create a Build resource, controlling the Pod generation in a namespace of their choice, including the operator namespace. This issue affects Apache Camel K: from 2.0.0 before 2.8.1, from 2.9.0 before 2.9.2, from 2.10.0 before 2.10.1. Users are recommended to upgrade to version 2.10.1 (or 2.8.1 or 2.9.2), which fixes the issue.	2026-05-21	8.1
CVE-2026-41091	microsoft - malware_protection_engine	Improper link resolution before file access ('link following') in Microsoft Defender allows an authorized attacker to elevate privileges locally.	2026-05-20	7.8
CVE-2026-42834	microsoft - windows_admin_center	Improper link resolution before file access ('link following') in Azure Portal Windows Admin Center allows an authorized attacker to elevate privileges locally.	2026-05-20	7.8

CVE-2026-43494	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net/rds: reset op_nents when zerocopy page pin fails When iov_iter_get_pages2() fails in rds_message_zcopy_from_user(),the pinned pages are released with put_page(), and rm->data.op_mmp_znotifier is cleared. But we fail to properly clear rm->data.op_nents. Later when rds_message_purge() is called from rds_sendmsg() the cleanup loop iterates over the incorrectly non zero number of op_nents and frees them again. Fix this by properly resetting op_nents when it should be in rds_message_zcopy_from_user().	2026-05-21	7.8
CVE-2026-43498	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: accel/ivpu: Disallow re-exporting imported GEM objects Prevent re-exporting of imported GEM buffers by adding a custom prime_handle_to_fd callback that checks if the object is imported and returns -EOPNOTSUPP if so. Re-exporting imported GEM buffers causes loss of buffer flags settings,leading to incorrect device access and data corruption.	2026-05-21	7.8
CVE-2026-43499	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: rtmutex: Use waiter::task instead of current in remove_waiter() remove_waiter() is used by the slowlock paths, but it is also used for proxy-lock rollback in rt_mutex_start_proxy_lock() when invoked from futex_requeue(). In the latter case waiter::task is not current, but remove_waiter() operates on current for the dequeue operation. That results in several problems: 1) the rbtree dequeue happens without waiter::task::pi_lock being held 2) the waiter task's pi_blocked_on state is not cleared, which leaves a dangling pointer primed for UAF around. 3) rt_mutex_adjust_prio_chain() operates on the wrong top priority waiter task Use waiter::task instead of current in all related operations in remove_waiter() to cure those problems. [tglx: Fixup rt_mutex_adjust_prio_chain(), add a comment and amend the changelog]	2026-05-21	7.8
CVE-2026-43502	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net/rds: handle zerocopy send cleanup before the message is queued A zerocopy send can fail after user pages have been pinned but before the message is attached to the sending socket. The purge path currently infers zerocopy state from rm->m_rs, so an unqueued message can be cleaned up as if it owned normal payload pages. However, zerocopy ownership is really determined by the presence of op_mmp_znotifier, regardless of whether the message has reached the socket queue. Capture op_mmp_znotifier up front in rds_message_purge() and use it as the cleanup discriminator. If the message is already associated with a socket, keep the existing completion path. Otherwise, drop the pinned page accounting directly and release the notifier before putting the payload pages. This keeps early send failure cleanup consistent with the zerocopy lifetime rules without changing the normal queued completion path.	2026-05-21	7.8
CVE-2025-71212	trendmicro - multiple products	A link following vulnerability in the Trend Micro Apex One scan engine could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2026-05-21	7.8
CVE-2025-71213	trendmicro - multiple products	An origin validation error vulnerability in Trend Micro Apex One could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2026-05-21	7.8
CVE-2026-34927	trendmicro - multiple products	An origin validation vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2026-05-21	7.8
CVE-2026-34928	trendmicro - multiple products	An origin validation vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. This is similar to CVE-2026-34927 but exists in a different named pipe communication mechanism. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2026-05-21	7.8
CVE-2026-34929	trendmicro - multiple products	An origin validation vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. This is similar to CVE-2026-34927 but exists in a different inter-process communication mechanism. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2026-05-21	7.8
CVE-2026-34930	trendmicro - multiple products	An origin validation vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. This is similar to CVE-2026-34927 but exists in a different process protection mechanism. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2026-05-21	7.8

CVE-2026-45206	trendmicro - multiple products	An origin validation vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. This is similar to CVE-2026-45207 but exists in a different process protection communication mechanism. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2026-05-21	7.8
CVE-2026-45207	trendmicro - multiple products	An origin validation vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. This is similar to CVE-2026-45206 but exists in a different process protection communication mechanism. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2026-05-21	7.8
CVE-2026-45208	trendmicro - multiple products	A time-of-check time-of-use vulnerability in the Apex One/SEP agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2026-05-21	7.8
CVE-2026-46300	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net: skbuff: preserve shared-frag marker during coalescing skb_try_coalesce() can attach paged frags from @from to @to. If @from has SKBFL_SHARED_FRAG set, the resulting @to skb can contain the same externally-owned or page-cache-backed frags, but the shared-frag marker is currently lost. That breaks the invariant relied on by later in-place writers. In particular, ESP input checks skb_has_shared_frag() before deciding whether an uncloned nonlinear skb can skip skb_cow_data(). If TCP receive coalescing has moved shared frags into an unmarked skb, ESP can see skb_has_shared_frag() as false and decrypt in place over page-cache backed frags. Propagate SKBFL_SHARED_FRAG when skb_try_coalesce() transfers paged frags. The tailroom copy path does not need the marker because it copies bytes into @to's linear data rather than transferring frag descriptors.	2026-05-23	7.8
CVE-2026-26147	microsoft - azure_stack_hci	Improper input validation in Azure Compute Gallery allows an authorized attacker to disclose information over a network.	2026-05-22	7.7
CVE-2026-42009	red hat - multiple products	A flaw was found in gnutls. A remote attacker could exploit an issue in the Datagram Transport Layer Security (DTLS) packet reordering logic. The comparator function, responsible for ordering DTLS packets by sequence numbers, did not correctly handle packets with duplicate sequence numbers. This could lead to unstable packet ordering or undefined behavior, resulting in a denial of service.	2026-05-18	7.5
CVE-2026-31909	apache - ofbiz	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	2026-05-19	7.5
CVE-2026-31910	apache - ofbiz	Server-Side Request Forgery (SSRF) vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	2026-05-19	7.5
CVE-2026-7307	red hat - multiple products	A flaw was found in Keycloak. A remote, unauthenticated attacker can send a specially crafted XML input to the Security Assertion Markup Language (SAML) endpoint. This malicious input can cause high CPU usage and worker thread starvation, leading to a Denial of Service (DoS) where the server becomes unavailable.	2026-05-19	7.5
CVE-2026-7507	red hat - multiple products	A session fixation vulnerability was found in Keycloak's login-actions endpoints. An unauthenticated attacker could exploit this flaw by pre-creating an authentication session and tricking a victim into visiting a maliciously crafted link. By leveraging the /login-actions/restart endpoint—which processes session handles without adequate CSRF protection or cookie ownership validation—an attacker can reset the authentication flow state. This causes Single Sign-On (SSO) to authenticate the victim transparently upon clicking the link, allowing the attacker to hijack the required-action form without needing the victim's credentials. A successful exploit could lead to complete account takeover, including highly privileged administrative accounts.	2026-05-19	7.5
CVE-2026-8945	mozilla - multiple products	Sandbox escape in Firefox and Firefox Focus for Android. This vulnerability was fixed in Firefox 151.	2026-05-19	7.5
CVE-2026-8946	mozilla - multiple products	Incorrect boundary conditions in the Audio/Video: Web Codecs component. This vulnerability was fixed in Firefox 151, Firefox ESR 115.36, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	2026-05-19	7.5
CVE-2026-8949	mozilla - multiple products	Integer overflow in the Widget: Win32 component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	2026-05-19	7.5
CVE-2026-8954	mozilla - multiple products	Incorrect boundary conditions, integer overflow in the Audio/Video component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	2026-05-19	7.5
CVE-2026-8960	mozilla - multiple products	Spoofing issue in WebExtensions. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	2026-05-19	7.5
CVE-2026-8963	mozilla - multiple products	Spoofing issue in the Web Speech component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	2026-05-19	7.5
CVE-2026-8964	mozilla - multiple products	Spoofing issue in the Popup Blocker component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	2026-05-19	7.5
CVE-2026-8965	mozilla - multiple products	Information disclosure in the DOM: Security component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	2026-05-19	7.5

CVE-2026-8966	mozilla - multiple products	Information disclosure in the IP Protection component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	2026-05-19	7.5
CVE-2026-8967	mozilla - multiple products	Information disclosure in the Graphics: WebGPU component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	2026-05-19	7.5
CVE-2026-8968	mozilla - multiple products	Denial-of-service due to invalid pointer in the Audio/Video: Web Codecs component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	2026-05-19	7.5
CVE-2026-9064	red hat - multiple products	A flaw was found in 389-ds-base. The get_ldapmessage_controls_ext() function in the LDAP server does not enforce an upper bound on the number of controls per LDAP message. A remote, unauthenticated attacker can send a specially crafted LDAP request containing hundreds of thousands of minimal controls within the default maximum BER message size (2 MB), causing excessive CPU consumption and heap allocation on the server. Under concurrent exploitation, this leads to significant latency degradation, worker thread starvation, or out-of-memory termination, resulting in a denial of service.	2026-05-20	7.5
CVE-2025-32750	dell - multiple products	Dell PowerFlex Manager, version(s) <=4.6.2, contain(s) an Exposure of Information Through Directory Listing vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	2026-05-20	7.5
CVE-2026-9117	google - chrome	Type Confusion in GFX in Google Chrome on Linux, ChromeOS prior to 148.0.7778.179 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted video file. (Chromium security severity: High)	2026-05-20	7.5
CVE-2026-9123	google - chrome	Heap buffer overflow in Chromecast in Google Chrome on Android, Linux, ChromeOS prior to 148.0.7778.179 allowed a local attacker to execute arbitrary code inside a sandbox via malicious network traffic. (Chromium security severity: Medium)	2026-05-20	7.5
CVE-2026-44417	apache - multiple products	The fix for CVE-2025-48913: Apache CXF: Untrusted JMS configuration can lead to RCE was not complete, meaning that another path in the code might lead to code execution capabilities, if untrusted users are allowed to configure JMS for Apache CXF. Users are recommended to upgrade to versions 4.2.1, 4.1.6 or 3.6.11, which fix this issue.	2026-05-22	7.5
CVE-2026-23663	microsoft - global_secure_access	Improper privilege management in Azure Entra ID allows an unauthorized attacker to elevate privileges over a network.	2026-05-22	7.5
CVE-2026-29226	apache - ofbiz	Server-Side Request Forgery (SSRF) vulnerability in Apache OFBiz via Content component operations. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	2026-05-19	7.3
CVE-2026-8947	mozilla - multiple products	Use-after-free in the DOM: Bindings (WebIDL) component. This vulnerability was fixed in Firefox 151, Firefox ESR 115.36, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	2026-05-19	7.3
CVE-2026-29518	samba - rsync	Rsync versions before 3.4.3 contain a time-of-check to time-of-use (TOCTOU) race condition in daemon file handling that allows attackers to redirect file writes outside intended directories by replacing parent directory components with symbolic links. Attackers with write access to a module path can exploit this race condition to create or overwrite arbitrary files, potentially modifying sensitive system files and achieving privilege escalation when the daemon runs with elevated privileges. This vulnerability can only be triggered if the chroot setting is false.	2026-05-20	7.3
CVE-2026-43497	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: fbdev: udlfb: add vm_ops to dlfb_ops_mmap to prevent use-after-free dlfb_ops_mmap() uses remap_pfn_range() to map vmalloc framebuffer pages to userspace but sets no vm_ops on the VMA. This means the kernel cannot track active mmaps. When dlfb_realloc_framebuffer() replaces the backing buffer via FBIOPUT_VSCREENINFO, existing mmap PTEs are not invalidated. On USB disconnect, dlfb_ops_destroy() calls vfree() on the old pages while userspace PTEs still reference them, resulting in a use-after-free: the process retains read/write access to freed kernel pages. Add vm_operations_struct with open/close callbacks that maintain an atomic mmap_count on struct dlfb_data. In dlfb_realloc_framebuffer(), check mmap_count and return -EBUSY if the buffer is currently mapped, preventing buffer replacement while userspace holds stale PTEs. Tested with PoC using dummy_hcd + raw_gadget USB device emulation.	2026-05-21	7.3
CVE-2026-43619	samba - rsync	Rsync version 3.4.2 and prior contain symlink race condition vulnerabilities in path-based system calls including chmod, lchown, utimes, rename, unlink, mkdir, symlink, mknod, link, rmdir, and lstat that allow local attackers to redirect operations to files outside the exported rsync module. Attackers with local filesystem access can exploit the timing window between path resolution and syscall execution by swapping symlinks to apply sender-supplied permissions, ownership, timestamps, or filenames to arbitrary files outside the intended module boundary on rsync daemons configured with 'use chroot = no'.	2026-05-20	7.2
CVE-2026-7571	red hat - multiple products	A flaw was found in Keycloak. A low-privilege user, with knowledge of user credentials and client ID, can bypass a security control intended to disable the implicit flow in OpenID Connect (OIDC) clients. By manipulating client data during a session restart, an attacker can obtain an access token that should not be available. This vulnerability can also lead to the exposure of these access tokens in server logs, proxy logs, and HTTP Referrer headers, resulting in sensitive information disclosure.	2026-05-19	7.1
CVE-2026-43620	samba - rsync	Rsync version 3.4.2 and prior contain a receiver-side out-of-bounds array read vulnerability in recv_files() in receiver.c that allows a malicious rsync server to crash the rsync client process. Attackers can exploit the vulnerability by setting CF_INC_RECURSE in compatibility flags and sending a specially crafted file list where the first sorted entry is not the leading dot directory, followed by a transfer record with ndx=0 and an iflag word without ITEM_TRANSFER, causing the receiver to read 8 bytes before the allocated pointer array and dereference an invalid pointer at an unmapped address, resulting in a deterministic SIGSEGV crash of the rsync client.	2026-05-20	6.9

CVE-2026-41119	dell - Live Optics	Dell Live Optics Windows and Personal Edition collectors contain an improper certificate validation vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability leading to loss of confidentiality and integrity.	2026-05-18	6.8
CVE-2026-37982	red hat - multiple products	A flaw was found in Keycloak. This authentication vulnerability allows a remote attacker to replay `ExecuteActionsActionToken` tokens within Keycloak's WebAuthn (Web Authentication) flow. By intercepting an execute-actions email link, an attacker can register their own authenticator to a victim's account. This leads to unauthorized enrollment of a hardware-backed credential, enabling persistent account takeover.	2026-05-19	6.8
CVE-2026-4630	red hat - multiple products	A flaw was found in Keycloak. An authenticated client could exploit an Insecure Direct Object Reference (IDOR) vulnerability in the Authorization Services Protection API endpoint. By knowing or obtaining a resource's unique identifier (UUID) belonging to another Resource Server within the same realm, the client could bypass authorization checks. This allows the client to perform unauthorized GET, PUT, and DELETE operations on resources, leading to information disclosure and potential unauthorized modification or deletion of data.	2026-05-19	6.8
CVE-2026-45585	microsoft - multiple products	Microsoft is aware of a security feature bypass vulnerability in Windows publicly referred to as "YellowKey". The proof of concept for this vulnerability has been made public violating coordinated vulnerability best practices. We are issuing this CVE to provide mitigation guidance that can be implemented to protect against this vulnerability until the security update is made available. Mitigation FAQs Should I leverage the temporary mitigation? Microsoft recommends that you consider implementing these mitigations if you are concerned your devices and data are at risk of being compromised or stolen. For example, if your organization’s employees take their work devices home or on business travel. What impact to service availability/management could be caused by implementing the mitigations? Implementing these mitigations will not impact service availability or management operations. Do customers need to revert the changes made to mitigate the vulnerability once the security update to protect against this vulnerability is available? No. The security update will maintain the mitigation's behavior once the security update is installed. I am using TPM+PIN, am I at risk of this vulnerability being exploited No, if you are using TPM+PIN the vulnerability is not exploitable.	2026-05-20	6.8
CVE-2026-20171	cisco - Cisco NX-OS Software	A vulnerability in the Border Gateway Protocol (BGP) enforce-first-as feature of Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an unauthenticated, remote attacker to trigger BGP peer flaps, resulting in a denial of service (DoS) condition. This vulnerability is due to incorrect parsing of a transitive BGP attribute. An attacker could exploit this vulnerability by sending a crafted BGP update through an established BGP peer session. If the update propagates to an affected device, it could cause the device to drop the BGP session and flap with the BGP peer that is forwarding this update, resulting in a DoS condition.	2026-05-20	6.8
CVE-2026-34926	trendmicro - multiple products	A directory traversal vulnerability in the Apex One (on-premise) server could allow a pre-authenticated local attacker to modify a key table on the server to inject malicious code to deploy to agents on affected installations. This vulnerability is only exploitable on the on-premise version of Apex One and a potential attacker must have access to the Apex One Server and already obtained administrative credentials to the server via some other method to exploit this vulnerability.	2026-05-21	6.7
CVE-2021-21508	dell - VxRail	Dell VxRail versions before 7.0.200 contain a Plain-text Password Storage Vulnerability in VxRail Manager. A sys-admin user may exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	2026-05-22	6.7
CVE-2026-6366	drupal - multiple products	Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal Drupal core allows Object Injection. This issue affects Drupal core: from 8.0.0 before 10.5.9, from 10.6.0 before 10.6.7, from 11.0.0 before 11.2.11, from 11.3.0 before 11.3.7.	2026-05-19	6.6
CVE-2026-20685	apple - Private Cloud Compute Server Software	An attacker in a privileged network position may be able to leak sensitive information. A path handling issue was addressed with improved validation. This issue is fixed in PCC Release 5E290.3.	2026-05-18	6.5
CVE-2026-29207	apache - ofbiz	Improper Neutralization of Special Elements Used in a Template Engine vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue. Please note that in the updated version, "Data Resource" records with dataTemplateTypeId = "FTL" are no longer supported. Additionally, in the updated version, the "Ecommerce Customer" security group no longer includes content management grants. Users are advised to remove these permissions from any production site as well.	2026-05-19	6.5
CVE-2026-29220	apache - ofbiz	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	2026-05-19	6.5

CVE-2026-31378	apache - ofbiz	Improper Input Validation vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	2026-05-19	6.5
CVE-2026-31380	apache - ofbiz	Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	2026-05-19	6.5
CVE-2026-35086	apache - ofbiz	Improper Control of Generation of Code ('Code Injection') vulnerability in email services of Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	2026-05-19	6.5
CVE-2026-45187	apache - ofbiz	Improper Authorization vulnerability in Apache OFBiz Webtools. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	2026-05-19	6.5
CVE-2026-37979	red hat - multiple products	A flaw was found in Keycloak. This access control vulnerability in Keycloak's OpenID Connect (OIDC) token introspection endpoint allows a confidential client to bypass audience restrictions. An attacker-controlled client with valid credentials can retrieve sensitive token claims intended for other resource servers, compromising the confidentiality of lightweight access tokens. This issue can be exploited remotely by any confidential client in the realm with valid credentials.	2026-05-19	6.5
CVE-2026-8951	mozilla - firefox	Spoofing issue in the Toolbar component in Firefox for Android. This vulnerability was fixed in Firefox 151.	2026-05-19	6.5
CVE-2026-8961	mozilla - multiple products	Spoofing issue in the Form Autofill component. This vulnerability was fixed in Firefox 151, Firefox ESR 140.11, Thunderbird 151, and Thunderbird 140.11.	2026-05-19	6.5
CVE-2026-8971	mozilla - multiple products	Same-origin policy bypass in the Networking: JAR component. This vulnerability was fixed in Firefox 151 and Thunderbird 151.	2026-05-19	6.5
CVE-2026-8706	mozilla - firefox	Firefox for iOS hosted Reader mode on an unauthenticated local web server, allowing another application on the same device to request arbitrary URLs and receive the response rendered with the signed-in user's cookies. This vulnerability was fixed in Firefox for iOS 151.0.	2026-05-19	6.5
CVE-2026-44923	veritas - infoscale_operations_manager	SQL injection in InfoScale VIOM before v9.1.3 allows remote attackers to escalate privileges.	2026-05-20	6.5
CVE-2026-9122	google - chrome	Out of bounds read in GPU in Google Chrome on Mac prior to 148.0.7778.179 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-05-20	6.5
CVE-2026-9150	red hat - multiple products	A flaw was found in libsolv. This stack-based buffer overflow vulnerability occurs in libsolv's Debian metadata parser when processing specially crafted Debian repository metadata. An attacker could exploit this by providing malicious SHA384 or SHA512 checksum tags, leading to memory corruption and a denial of service (DoS) in the affected system.	2026-05-20	6.5
CVE-2026-9149	red hat - multiple products	A flaw was found in libsolv. This heap buffer overflow vulnerability occurs when a victim processes a specially crafted `.solv` file containing negative size values in the `repo_add_solv` function. This leads to an undersized memory allocation and a subsequent out-of-bounds write. An attacker could exploit this to cause a denial of service (DoS).	2026-05-21	6.5
CVE-2022-34363	dell - unisphere_for_powermax_virtual_appliance	Dell Unisphere for PowerMax vApp version prior to 10.0.0.2, contains an authorization bypass vulnerability in the Unisphere for VMAX application running in vApp	2026-05-22	6.5
CVE-2026-42827	microsoft - 365_copilot	Improper neutralization of special elements used in a command ('command injection') in M365 Copilot allows an unauthorized attacker to disclose information over a network.	2026-05-22	6.5
CVE-2026-35070	dell - smartfabric_storage_software	Dell SmartFabric Storage Software, versions prior to 1.4.5, contains an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Filesystem access for attacker.	2026-05-20	6.4
CVE-2026-9087	red hat - Red Hat Build of Keycloak	A flaw was found in Keycloak. The cross-session verification proof is keyed only by (local userId, idpAlias) and is not bound to the upstream identity that was actually verified, so a second upstream account on the same IdP can consume it and get linked to the victim's local account.	2026-05-20	6.4
CVE-2026-43617	samba - rsync	Rsync version 3.4.2 and prior contain an authorization bypass vulnerability in the rsync daemon's hostname-based access control list enforcement when configured with chroot. Attackers can bypass hostname-based deny rules by controlling the PTR record for their source IP address, allowing connections from hostnames that administrators intended to deny when reverse DNS resolution fails and defaults to UNKNOWN.	2026-05-20	6.3
CVE-2026-20206	cisco - Cisco ThousandEyes Enterprise Agent	A vulnerability in the BrowserBot component of Cisco ThousandEyes Enterprise Agent could have allowed an authenticated, remote attacker to execute arbitrary commands on Agents on behalf of the BrowserBot synthetics orchestration process. Cisco has addressed this vulnerability in the Cisco ThousandEyes Enterprise Agent, and no customer action is needed. This vulnerability was due to insufficient input validation of command arguments that are supplied by the user. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by authenticating to the ThousandEyes SaaS and submitting crafted input into the affected parameter. A successful exploit could have allowed the attacker to execute arbitrary commands within the BrowserBot container as the node user. To exploit this vulnerability, the attacker must have valid user credentials for the ThousandEyes SaaS and the ability to manage transaction tests.	2026-05-20	6.3

CVE-2026-31379	apache - ofbiz	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Control of Generation of Code ('Code Injection') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	2026-05-19	6.1
CVE-2026-31906	apache - ofbiz	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	2026-05-19	6.1
CVE-2026-6365	drupal - multiple products	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Drupal core allows Cross-Site Scripting (XSS). This issue affects Drupal core: from 8.0.0 before 10.5.9, from 10.6.0 before 10.6.7, from 11.0.0 before 11.2.11, from 11.3.0 before 11.3.7.	2026-05-19	6.1
CVE-2026-6367	drupal - drupal	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Drupal core allows Cross-Site Scripting (XSS). This issue affects Drupal core: from 11.3.0 before 11.3.7.	2026-05-19	6.1
CVE-2026-43618	samba - rsync	Rsync version 3.4.2 and prior contain an integer overflow vulnerability in the compressed-token decoder where a 32-bit signed counter is not checked for overflow, allowing a malicious sender to trigger an overflow that causes the receiver process to read and return data from outside the intended buffer bounds. Attackers can exploit this vulnerability to disclose process memory contents including environment variables, passwords, heap and stack data, and library memory pointers, significantly reducing ASLR effectiveness and facilitating further exploitation.	2026-05-20	6.1
CVE-2025-26483	dell - multiple products	Dell PowerFlex Manager, versions 4.6.2 and prior, contains an Open Redirect Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability, leading to a targeted application user being redirected to arbitrary web URLs. The vulnerability could be leveraged by attackers to conduct phishing attacks that cause users to divulge sensitive information.	2026-05-22	6.1
CVE-2022-31231	dell - multiple products	Dell ECS, versions 3.5 and 3.6, contain an Improper Access Control in the Identity and Access Management (IAM) module. A remote unauthenticated attacker may potentially exploit this vulnerability, leading to gaining read access to unauthorized data.	2026-05-22	5.9
CVE-2025-32751	dell - multiple products	Dell PowerFlex Manager, version(s) <=4.6.2, contain(s) an Insecure Storage of Sensitive Information vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to unauthorized access to sensitive information.	2026-05-22	5.5
CVE-2026-45492	microsoft - edge_chromium	Improper input validation in Microsoft Edge (Chromium-based) allows an unauthorized attacker to bypass a security feature over a network.	2026-05-18	5.4
CVE-2026-45494	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2026-05-18	5.4
CVE-2026-8922	red hat - Red Hat Build of Keycloak	A flaw was found in Keycloak. When both realm-level and client-level `notBefore` revocation policies are configured, Keycloak's OpenID Connect (OIDC) Introspection feature fails to properly honor the realm-level policy. This allows tokens that should have been revoked to remain active, potentially leading to unauthorized access or continued session validity. This could impact the security of systems utilizing Keycloak for identity and access management.	2026-05-19	5.4
CVE-2026-44924	veritas - infoscale_operations_manager	InfoScale VIOM 9.1.3 allows XSS.	2026-05-20	5.4
CVE-2026-8381	teamviewer - DEX (On-premises)	A broken access control vulnerability exists in the TeamViewer DEX Platform (On-Premises) prior version 9.2. Certain backend API endpoints do not correctly enforce authorization checks, allowing an authenticated user with low privileges to perform actions and access resources intended only for higher-privileged roles. An attacker with low-privileged credentials may exploit this to gain unauthorized access to administrative or sensitive functionality.	2026-05-22	5.4
CVE-2018-25321	tp-link - tl-wr720n_firmware	TP-Link TL-WR720N wireless router contains a cross-site request forgery vulnerability that allows attackers to perform unauthorized administrative actions by crafting malicious web requests. Attackers can modify port forwarding rules via VirtualServerRpm.htm or change WiFi security settings via WlanSecurityRpm.htm by tricking authenticated users into visiting attacker-controlled pages.	2026-05-17	5.3
CVE-2026-31387	apache - ofbiz	Improper Authentication vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	2026-05-19	5.3
CVE-2026-31388	apache - ofbiz	Improper Access Control vulnerability in Apache OFBiz in multi-tenant deployments. This issue affects Apache OFBiz: before 24.09.06. Users are recommended to upgrade to version 24.09.06, which fixes the issue.	2026-05-19	5.3
CVE-2026-42526	apache software foundation - Apache Airflow Amazon provider	In the AWS Secrets Manager and SSM Parameter Store secrets backends of `apache-airflow-providers-amazon` prior to 9.28.0, the team-scoping logic could resolve a `conn_id` containing a `/` (e.g. `"my_team/conn"`) to the same path as another team's team-scoped secret when the caller had no team context. A privileged caller without team context could therefore retrieve another team's secret by crafting a colliding `conn_id`. Fixed in 9.28.0 by switching the team-scope separator to `--` and rejecting team-shaped `conn_id`s when team context is absent. Affects the experimental multi-tenant teams feature only. Users are recommended to upgrade to `apache-airflow-providers-amazon` 9.28.0, which fixes the issue.	2026-05-19	5.3
CVE-2026-9124	google - chrome	Insufficient validation of untrusted input in Input in Google Chrome on prior to 148.0.7778.179 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-05-20	5.3
CVE-2026-44618	apache - multiple products	Insecure XML parser configuration in Apache CXF's WS-Transfer module may allow attackers to perform XXE attacks. Users are recommended to upgrade to versions 4.2.1, 4.1.6 or 3.6.11, which fix this issue.	2026-05-22	5.3
CVE-2025-32747	dell - multiple products	Dell PowerFlex Manager, version(s) <=4.6.2, contain(s) an Incorrect Privilege Assignment vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	2026-05-22	5.3

CVE-2025-32749	dell - multiple products	Dell PowerFlex Manager, version(s) <=4.6.2, contain(s) an Exposure of Information Through Directory Listing vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	2026-05-22	5.3
CVE-2026-4093	drupal - Term Reference Tree	In the Drupal 7 Term Reference Tree module, two stored XSS vectors exist in the widget/formatter rendering pipeline. Vector A (token display templates): When the Token module is enabled and token display templates are configured, attacker-controlled token output (e.g., term description) is rendered without proper sanitization. Any user who can edit the referenced taxonomy terms can inject HTML/JS that executes when the field is rendered. Vector B (term label rendering): Taxonomy term labels are not properly sanitized before being rendered in the widget, allowing a user with permission to create or edit taxonomy terms to inject scripts into the term name that execute when a form containing the widget is viewed. Exploit affects versions 7.x-1.x up to and including 7.x-1.11.	2026-05-21	5.1
CVE-2026-4929	drupal - Simple Hierarchical Select (shs)	Simple Hierarchical Select (SHS) for Drupal 7 contains cross-site scripting risk due to improper output escaping of term-derived text. Confirmed affected paths include field formatter output (shs_field_formatter_view) and term-tree child-term data generation (shs_term_get_children). Malicious taxonomy term names can be rendered unsafely depending on output context. This affects versions from 7.x-1.0 through (and including) 7.x-1.10.	2026-05-21	5.1
CVE-2026-37978	red hat - multiple products	A flaw was found in Keycloak. A low-privilege administrator with the 'view-clients' role can exploit this by invoking the 'evaluate-scopes' Admin API endpoints with an arbitrary user ID (userId) parameter. This vulnerability allows for cross-role personally identifiable information (PII) leakage, enabling unauthorized visibility into user identities and authorizations across the realm. Exploitation is possible remotely via network access to the Admin API.	2026-05-19	4.9
CVE-2026-20199	cisco - Cisco ThousandEyes Enterprise Agent	A vulnerability in the SSL certificate handling of Cisco ThousandEyes Virtual Appliance could allow an authenticated, remote attacker to execute commands on the underlying operating system as the root user. This vulnerability is due to insufficient validation of user-supplied input. An authenticated attacker could exploit this vulnerability by uploading a crafted certificate to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system. To exploit this vulnerability, the attacker must have valid administrative credentials.	2026-05-20	4.7
CVE-2026-8830	red hat - Red Hat Build of Keycloak	A flaw was found in Keycloak. An authenticated user can bypass configured WebAuthn policies during credential registration by manipulating client-side JavaScript. This occurs because the server-side processAction() fails to validate that the newly created credential's parameters, such as public key algorithms, match the realm's configured WebAuthn policies. This could lead to the creation of credentials that do not adhere to administrative security requirements, potentially weakening the overall security posture of the system by allowing non-compliant authentication methods.	2026-05-19	4.3
CVE-2026-37981	red hat - multiple products	A flaw was found in Keycloak. A broken access control vulnerability in the Account Resources user lookup endpoint allows a remote authenticated user, who owns at least one User-Managed Access (UMA) resource, to enumerate and harvest personally identifiable information (PII) for all realm users. By sending crafted requests with arbitrary usernames or email values, the endpoint returns full profile objects for unrelated users. This leads to broad profile-level information disclosure.	2026-05-19	4.3
CVE-2026-9113	google - chrome	Out of bounds read in GPU in Google Chrome on Mac prior to 148.0.7778.179 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	2026-05-20	4.3
CVE-2026-9115	google - chrome	Insufficient policy enforcement in Service Worker in Google Chrome on prior to 148.0.7778.179 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: High)	2026-05-20	4.3
CVE-2026-9116	google - chrome	Insufficient policy enforcement in ServiceWorker in Google Chrome on prior to 148.0.7778.179 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-05-20	4.3
CVE-2026-9110	google - chrome	Inappropriate implementation in UI in Google Chrome on Windows prior to 148.0.7778.179 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Critical)	2026-05-20	4.2
CVE-2025-32745	dell - multiple products	Dell PowerFlex Manager, version(s) <=4.6.2, contain(s) an Improper Certificate Validation vulnerability. An unauthenticated attacker with adjacent network access could potentially exploit this vulnerability, leading to Information tampering.	2026-05-22	4.2
CVE-2026-45498	microsoft - defender_antimalware_platform	Microsoft Defender Denial of Service Vulnerability	2026-05-20	4.0
CVE-2025-32746	dell - multiple products	Dell PowerFlex Manager, version(s) <=4.6.2, contain(s) an Insecure Storage of Sensitive Information vulnerability. An unauthenticated attacker with local access could potentially exploit this vulnerability, leading to unauthorized access to sensitive information.	2026-05-22	4.0
CVE-2025-46371	dell - multiple products	Dell PowerFlex Manager, version(s) <=4.6.2, contain(s) a Use of a Broken or Risky Cryptographic Algorithm vulnerability in the ssh. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Protection mechanism bypass.	2026-05-22	3.6
CVE-2026-45232	samba - rsync	Rsync versions before 3.4.3 contain an off-by-one out-of-bounds stack write vulnerability in the establish_proxy_connection() function in socket.c that allows network attackers to corrupt stack memory by sending a malformed HTTP proxy response. Attackers can exploit this by positioning themselves between the client and proxy or controlling the proxy server to send a response line of 1023 or more bytes without a newline terminator, causing a null byte to be written to an out-of-bounds stack address when the RSYNC_PROXY environment variable is set.	2026-05-20	2.1

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

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