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

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

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ١٩ يناير إلى ٢٥ يناير. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 19th of January to 25th of January. 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-2025-20156 | cisco - Cisco Meeting Management | A vulnerability in the REST API of Cisco Meeting Management could allow a remote, authenticated attacker with low privileges to elevate privileges to administrator on an affected device._x000D_ _x000D_ This vulnerability exists because proper authorization is not enforced upon REST API users. An attacker could exploit this vulnerability by sending API requests to a specific endpoint. A successful exploit could allow the attacker to gain administrator-level control over edge nodes that are managed by Cisco Meeting Management. | 2025-01-22 | 9.9 |
| CVE-2024-49747 | google - Android | In gatts_process_read_by_type_req of gatt_sr.cc, there is a possible out of bounds write due to a logic error in the code. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. | 2025-01-21 | 9.8 |
| CVE-2024-49748 | google - Android | In gatts_process_primary_service_req of gatt_sr.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. | 2025-01-21 | 9.8 |
| CVE-2025-23006 | sonicwall - sma8200v | Pre-authentication deserialization of untrusted data vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands. | 2025-01-23 | 9.8 |
| CVE-2024-38337 | ibm - Sterling Secure Proxy | IBM Sterling Secure Proxy 6.0.0.0, 6.0.0.1, 6.0.0.2, 6.0.0.3, 6.1.0.0, and 6.2.0.0 could allow an unauthorized attacker to retrieve or alter sensitive information contents due to incorrect permission assignments. | 2025-01-19 | 9.1 |
| CVE-2024-41783 | ibm - Sterling Secure Proxy | IBM Sterling Secure Proxy 6.0.0.0, 6.0.0.1, 6.0.0.2, 6.0.0.3, 6.1.0.0, and 6.2.0.0 could allow a privileged user to inject commands into the underlying operating system due to improper validation of a specified type of input. | 2025-01-19 | 9.1 |
| CVE-2024-45479 | apache software foundation - Apache Ranger | SSRF vulnerability in Edit Service Page of Apache Ranger UI in Apache Ranger Version 2.4.0. Users are recommended to upgrade to version Apache Ranger 2.5.0, which fixes this issue. | 2025-01-21 | 9.1 |
| CVE-2024-51941 | apache software foundation - Apache Ambari | A remote code injection vulnerability exists in the Ambari Metrics and AMS Alerts feature, allowing authenticated users to inject and execute arbitrary code. The vulnerability occurs when processing alert definitions, where malicious input can be injected into the alert script execution path. An attacker with authenticated access can exploit this vulnerability to execute arbitrary commands on the server. The issue has been fixed in the latest versions of Ambari. | 2025-01-21 | 8.8 |
| CVE-2025-23196 | apache software foundation - Apache Ambari | A code injection vulnerability exists in the Ambari Alert Definition feature, allowing authenticated users to inject and execute arbitrary shell commands. The vulnerability arises when defining alert scripts, where the script filename field is executed using `sh -c`. An attacker with authenticated access can exploit this vulnerability to inject malicious commands, leading to remote code execution on the server. The issue has been fixed in the latest versions of Ambari. | 2025-01-21 | 8.8 |
| CVE-2024-43096 | google - Android | In build_read_multi_rsp of gatt_sr.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation. | 2025-01-21 | 8.8 |

| | | | | |
|---|---|---|---|---|
| CVE-2024-43770 | google - Android | In gatts_process_find_info of gatt_sr.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation. | 2025-01-21 | 8.8 |
| CVE-2024-43771 | google - Android | In gatts_process_read_req of gatt_sr.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation. | 2025-01-21 | 8.8 |
| CVE-2024-49749 | google - Android | In DGifSlurp of dgif_lib.c, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. | 2025-01-21 | 8.8 |
| CVE-2024-31903 | ibm - Sterling B2B Integrator Standard Edition | IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.1.2.5 and 6.2.0.0 through 6.2.0.2 allow an attacker on the local network to execute arbitrary code on the system, caused by the deserialization of untrusted data. | 2025-01-22 | 8.8 |
| CVE-2024-41739 | ibm - Cognos Dashboards on Cloud Pak for Data | IBM Cognos Dashboards 4.0.7 and 5.0.0 on Cloud Pak for Data could allow a remote attacker to perform unauthorized actions due to dependency confusion. | 2025-01-24 | 8.8 |
| CVE-2024-39750 | ibm - Analytics Content Hub | IBM Analytics Content Hub 2.0 is vulnerable to a buffer overflow due to improper return length checking. A remote authenticated attacker could overflow a buffer and execute arbitrary code on the system or cause the server to crash. | 2025-01-25 | 8.8 |
| CVE-2024-11218 | red hat - multiple products | A vulnerability was found in `podman build` and `buildah.` This issue occurs in a container breakout by using --jobs=2 and a race condition when building a malicious Containerfile. SELinux might mitigate it, but even with SELinux on, it still allows the enumeration of files and directories on the host. | 2025-01-22 | 8.6 |
| CVE-2025-0650 | red hat - multiple products | A flaw was found in the Open Virtual Network (OVN). Specially crafted UDP packets may bypass egress access control lists (ACLs) in OVN installations configured with a logical switch with DNS records set on it and if the same switch has any egress ACLs configured. This issue can lead to unauthorized access to virtual machines and containers running on the OVN network. | 2025-01-23 | 8.1 |
| CVE-2024-25034 | ibm - Planning Analytics Local | IBM Planning Analytics 2.0 and 2.1 could be vulnerable to malicious file upload by not validating the type of file in the File Manager T1 process. Attackers can make use of this weakness and upload malicious executable files into the system that can be sent to victims for performing further attacks. | 2025-01-24 | 8 |
| CVE-2024-40693 | ibm - Planning Analytics Local | IBM Planning Analytics 2.0 and 2.1 could be vulnerable to malicious file upload by not validating the content of the file uploaded to the web interface. Attackers can make use of this weakness and upload malicious executable files into the system, and it can be sent to victim for performing further attacks. | 2025-01-24 | 8 |
| CVE-2024-57926 | linux - multiple products | In the Linux kernel, the following vulnerability has been resolved:<br><br>drm/mediatek: Set private->all_drm_private[i]->drm to NULL if mtk_drm_bind returns err<br><br>The pointer need to be set to NULL, otherwise KASAN complains about<br>use-after-free. Because in mtk_drm_bind, all private's drm are set<br>as follows.<br><br>private->all_drm_private[i]->drm = drm;<br><br>And drm will be released by drm_dev_put in case mtk_drm_kms_init returns<br>failure. However, the shutdown path still accesses the previous allocated<br>memory in drm_atomic_helper_shutdown.<br><br>[ 84.874820] watchdog: watchdog0: watchdog did not stop!<br>[ 86.512054] ==========<br>[ 86.513162] BUG: KASAN: use-after-free in drm_atomic_helper_shutdown+0x33c/0x378<br>[ 86.514258] Read of size 8 at addr ffff0000d46fc068 by task shutdown/1<br>[ 86.515213]<br>[ 86.515455] CPU: 1 UID: 0 PID: 1 Comm: shutdown Not tainted 6.13.0-rc1-mtk+gfa1a78e5d24b-dirty #55<br>[ 86.516752] Hardware name: Unknown Product/Unknown Product, BIOS 2022.10 10/01/2022<br>[ 86.517960] Call trace:<br>[ 86.518333] show_stack+0x20/0x38 (C)<br>[ 86.518891] dump_stack_lvl+0x90/0xd0<br>[ 86.519443] print_report+0xf8/0x5b0<br>[ 86.519985] kasan_report+0xb4/0x100<br>[ 86.520526] __asan_report_load8_noabort+0x20/0x30<br>[ 86.521240] drm_atomic_helper_shutdown+0x33c/0x378<br>[ 86.521966] mtk_drm_shutdown+0x54/0x80<br>[ 86.522546] platform_shutdown+0x64/0x90<br>[ 86.523137] device_shutdown+0x260/0x5b8<br>[ 86.523728] kernel_restart+0x78/0xf0<br>[ 86.524282] __do_sys_reboot+0x258/0x2f0<br>[ 86.524871] __arm64_sys_reboot+0x90/0xd8<br>[ 86.525473] invoke_syscall+0x74/0x268<br>[ 86.526041] el0_svc_common.constprop.0+0xb0/0x240<br>[ 86.526751] do_el0_svc+0x4c/0x70<br>[ 86.527251] el0_svc+0x4c/0xc0<br>[ 86.527719] el0t_64_sync_handler+0x144/0x168<br>[ 86.528367] el0t_64_sync+0x198/0x1a0<br>[ 86.528920]<br>[ 86.529157] The buggy address belongs to the physical page:<br>[ 86.529972] page: refcount:0 mapcount:0 mapping:0000000000000000 index:0xffff0000d46fd4d0 pfn:0x1146fc<br>[ 86.531319] flags: 0xbfffc0000000000(node=0\|zone=2\|lastcpupid=0xffff)<br>[ 86.532267] raw: 0bfffc0000000000 0000000000000000 dead000000000122 0000000000000000 | 2025-01-19 | 7.8 |

| | | | | |
|---|---|---|---|---|
| | | [ 86.533390] raw: ffff0000d46fd4d0 0000000000000000 00000000ffffffff 0000000000000000<br>[ 86.534511] page dumped because: kasan: bad access detected<br>[ 86.535323]<br>[ 86.535559] Memory state around the buggy address:<br>[ 86.536265] ffff0000d46fbf00: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff<br>[ 86.537314] ffff0000d46fbf80: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff<br>[ 86.538363] >ffff0000d46fc000: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff<br>[ 86.544733] ^<br>[ 86.551057] ffff0000d46fc080: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff<br>[ 86.557510] ffff0000d46fc100: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff<br>[ 86.563928] ==========<br>[ 86.571093] Disabling lock debugging due to kernel taint<br>[ 86.577642] Unable to handle kernel paging request at virtual address e0e9c0920000000b<br>[ 86.581834] KASAN: maybe wild-memory-access in range [0x0752049000000058-0x075204900000005f]<br>... | | |
| CVE-2023-40132 | google - Android | In setActualDefaultRingtoneUri of RingtoneManager.java, there is a possible way to bypass content providers read permissions due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. | 2025-01-21 | 7.8 |
| CVE-2024-34730 | google - Android | In multiple locations, there is a possible bypass of user consent to enabling new Bluetooth HIDs due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | 2025-01-21 | 7.8 |
| CVE-2024-43095 | google - Android | In multiple locations, there is a possible way to obtain any system permission due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. | 2025-01-21 | 7.8 |
| CVE-2024-43765 | google - Android | In multiple locations, there is a possible way to obtain access to a folder due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation. | 2025-01-21 | 7.8 |
| CVE-2024-49732 | google - Android | In multiple functions of CompanionDeviceManagerService.java, there is a possible way to grant permissions without user consent due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | 2025-01-21 | 7.8 |
| CVE-2024-49735 | google - Android | In multiple locations, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | 2025-01-21 | 7.8 |
| CVE-2024-49736 | google - Android | In onClick of MainClear.java, there is a possible way to trigger factory reset without explicit user consent due to a logic error in the code. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. | 2025-01-21 | 7.8 |
| CVE-2024-49737 | google - Android | In applyTaskFragmentOperation of WindowOrganizerController.java, there is a possible way to launch arbitrary activities as the system UID due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | 2025-01-21 | 7.8 |
| CVE-2024-49738 | google - Android | In writeInplace of Parcel.cpp, there is a possible out of bounds write. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | 2025-01-21 | 7.8 |
| CVE-2024-49742 | google - Android | In onCreate of NotificationAccessConfirmationActivity.java , there is a possible way to hide an app with notification access in Settings due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. | 2025-01-21 | 7.8 |
| CVE-2024-49744 | google - Android | In checkKeyIntentParceledCorrectly of AccountManagerService.java, there is a possible way to bypass parcel mismatch mitigation due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. | 2025-01-21 | 7.8 |
| CVE-2024-49745 | google - Android | In growData of Parcel.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. | 2025-01-21 | 7.8 |
| CVE-2024-41742 | ibm - TXSeries for Multiplatforms | IBM TXSeries for Multiplatforms 10.1 is vulnerable to a denial of service, caused by improper enforcement of the timeout on individual read operations. By conducting a slowloris-type attacks, a remote attacker could exploit this vulnerability to cause a denial of service. | 2025-01-19 | 7.5 |
| CVE-2024-41743 | ibm - TXSeries for Multiplatforms | IBM TXSeries for Multiplatforms 10.1 could allow a remote attacker to cause a denial of service using persistent connections due to improper allocation of resources. | 2025-01-19 | 7.5 |
| CVE-2025-23195 | apache software foundation - Apache Ambari | An XML External Entity (XXE) vulnerability exists in the Ambari/Oozie project, allowing an attacker to inject malicious XML entities. This vulnerability occurs due to insecure parsing of XML input using the `DocumentBuilderFactory` class without disabling external entity resolution. An attacker can exploit this vulnerability to read arbitrary files on the server or perform server-side request forgery (SSRF) attacks. The issue has been fixed in both Ambari 2.7.9 and the trunk branch. | 2025-01-21 | 7.5 |
| CVE-2024-49734 | google - Android | In multiple functions of ConnectivityService.java, there is a possible way for a Wi-Fi AP to determine what site a device has connected to through a VPN due to side channel information disclosure. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. | 2025-01-21 | 7.5 |
| CVE-2025-20165 | cisco - Cisco BroadWorks | A vulnerability in the SIP processing subsystem of Cisco BroadWorks could allow an unauthenticated, remote attacker to halt the processing of incoming SIP requests, resulting in a denial of service (DoS) condition._x000D_<br>_x000D_<br>This vulnerability is due to improper memory handling for certain SIP requests. An attacker could exploit this vulnerability by sending a high number of SIP requests to an affected system. A successful exploit could allow the attacker to exhaust the memory that was allocated to the Cisco BroadWorks | 2025-01-22 | 7.5 |

| | | | | |
|---|---|---|---|---|
| | | Network Servers that handle SIP traffic. If no memory is available, the Network Servers can no longer process incoming requests, resulting in a DoS condition that requires manual intervention to recover. | | |
| CVE-2024-49724 | google - Android | In multiple functions of AccountManagerService.java, there is a possible way to bypass permissions and launch protected activities due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. | 2025-01-21 | 7 |
| CVE-2024-45652 | ibm - Maximo Asset Management | IBM Maximo MXAPIASSET API 7.6.1.3 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. | 2025-01-19 | 6.5 |
| CVE-2024-43763 | google - Android | In build_read_multi_rsp of gatt_sr.cc, there is a possible denial of service due to a logic error in the code. This could lead to remote (proximal/adjacent) denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. | 2025-01-21 | 6.5 |
| CVE-2024-45077 | ibm - Maximo Asset Management | IBM Maximo Asset Management 7.6.1.3 MXAPIASSET API is vulnerable to unrestricted file upload which allows authenticated low privileged user to upload restricted file types with a simple method of adding a dot to the end of the file name if Maximo is installed on Windows operating system. | 2025-01-24 | 6.5 |
| CVE-2023-50309 | ibm - Sterling B2B Integrator Standard Edition | IBM Sterling B2B Integrator 6.0.0.0 through 6.1.2.5 and 6.2.0.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. | 2025-01-23 | 6.4 |
| CVE-2025-24529 | phpmyadmin - phpMyAdmin | An issue was discovered in phpMyAdmin 5.x before 5.2.2. An XSS vulnerability has been discovered for the Insert tab. | 2025-01-23 | 6.4 |
| CVE-2025-24530 | phpmyadmin - phpMyAdmin | An issue was discovered in phpMyAdmin 5.x before 5.2.2. An XSS vulnerability has been discovered for the check tables feature. A crafted table or database name could be used for XSS. | 2025-01-23 | 6.4 |
| CVE-2025-23227 | ibm - Tivoli Application Dependency Discovery Manager | IBM Tivoli Application Dependency Discovery Manager 7.3.0.0 through 7.3.0.11 is vulnerable to stored cross-site scripting. This vulnerability allows authenticated users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. | 2025-01-23 | 6.4 |
| CVE-2024-35148 | ibm - Maximo Application Suite | IBM Maximo Application Suite 8.10.10, 8.11.7, and 9.0 - Monitor Component is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. | 2025-01-25 | 6.3 |
| CVE-2024-45091 | ibm - multiple products | IBM UrbanCode Deploy (UCD) 7.0 through 7.0.5.24, 7.1 through 7.1.2.10, and 7.2 through 7.2.3.13 stores potentially sensitive information in log files that could be read by a local user with access to HTTP request logs. | 2025-01-21 | 6.2 |
| CVE-2024-35145 | ibm - Maximo Application Suite | IBM Maximo Application Suite 9.0.0 - Monitor Component is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. | 2025-01-25 | 6.1 |
| CVE-2024-45672 | ibm - Security Verify Bridge | IBM Security Verify Bridge 1.0.0 through 1.0.15 could allow a local privileged user to overwrite files due to excessive privileges granted to the agent. which could also cause a denial of service. | 2025-01-23 | 6 |
| CVE-2024-22347 | ibm - multiple products | IBM DevOps Velocity 5.0.0 and IBM UrbanCode Velocity 4.0.0 through 4.0. 25 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. | 2025-01-20 | 5.9 |
| CVE-2025-23184 | apache software foundation - Apache CXF | A potential denial of service vulnerability is present in versions of Apache CXF before 3.5.10, 3.6.5 and 4.0.6. In some edge cases, the CachedOutputStream instances may not be closed and, if backed by temporary files, may fill up the file system (it applies to servers and clients). | 2025-01-21 | 5.9 |
| CVE-2024-41757 | ibm - Concert Software | IBM Concert Software 1.0.0 and 1.0.1 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. | 2025-01-24 | 5.9 |
| CVE-2024-45647 | ibm - multiple products | IBM Security Verify Access 10.0.0 through 10.0.8 and IBM Security Verify Access Docker 10.0.0 through 10.0.8 could allow could an unverified user to change the password of an expired user without prior knowledge of that password. | 2025-01-20 | 5.6 |
| CVE-2025-21644 | linux - multiple products | In the Linux kernel, the following vulnerability has been resolved:<br><br>drm/xe: Fix tlb invalidation when wedging<br><br>If GuC fails to load, the driver wedges, but in the process it tries to<br>do stuff that may not be initialized yet. This moves the<br>xe_gt_tlb_invalidation_init() to be done earlier: as its own doc says,<br>it's a software-only initialization and should had been named with the<br>_early() suffix.<br><br>Move it to be called by xe_gt_init_early(), so the locks and seqno are<br>initialized, avoiding a NULL ptr deref when wedging:<br><br>xe 0000:03:00.0: [drm] *ERROR* GT0: load failed: status: Reset = 0, BootROM = 0x50, UKernel = 0x00, MIA = 0x00, Auth = 0x01<br>xe 0000:03:00.0: [drm] *ERROR* GT0: firmware signature verification failed<br>xe 0000:03:00.0: [drm] *ERROR* CRITICAL: Xe has declared device 0000:03:00.0 as wedged.<br>...<br>BUG: kernel NULL pointer dereference, address: 0000000000000000<br>#PF: supervisor read access in kernel mode<br>#PF: error_code(0x0000) - not-present page<br>PGD 0 P4D 0<br>Oops: Oops: 0000 [#1] PREEMPT SMP NOPTI<br>CPU: 9 UID: 0 PID: 3908 Comm: modprobe Tainted: G U W 6.13.0-rc4-xe+ #3<br>Tainted: [U]=USER, [W]=WARN<br>Hardware name: Intel Corporation Alder Lake Client Platform/AlderLake-S ADP-S DDR5 UDIMM CRB, BIOS ADLSFWI1.R00.3275.A00.2207010640 07/01/2022<br>RIP: 0010:xe_gt_tlb_invalidation_reset+0x75/0x110 [xe] | 2025-01-19 | 5.5 |

| | | | | |
|---|---|---|---|---|
| | | This can be easily triggered by poking the GuC binary to force a<br>signature failure. There will still be an extra message,<br><br>xe 0000:03:00.0: [drm] *ERROR* GT0: GuC mmio request 0x4100: no reply 0x4100<br><br>but that's better than a NULL ptr deref.<br><br>(cherry picked from commit 5001ef3af8f2c972d6fd9c5221a8457556f8bea6) | | |
| CVE-2025-21649 | linux - multiple products | In the Linux kernel, the following vulnerability has been resolved:<br><br>net: hns3: fix kernel crash when 1588 is sent on HIP08 devices<br><br>Currently, HIP08 devices does not register the ptp devices, so the<br>hdev->ptp is NULL. But the tx process would still try to set hardware time<br>stamp info with SKBTX_HW_TSTAMP flag and cause a kernel crash.<br><br>[ 128.087798] Unable to handle kernel NULL pointer dereference at virtual address<br>0000000000000018<br>...<br>[ 128.280251] pc : hclge_ptp_set_tx_info+0x2c/0x140 [hclge]<br>[ 128.286600] lr : hclge_ptp_set_tx_info+0x20/0x140 [hclge]<br>[ 128.292938] sp : ffff800059b93140<br>[ 128.297200] x29: ffff800059b93140 x28: 0000000000003280<br>[ 128.303455] x27: ffff800020d48280 x26: ffff0cb9dc814080<br>[ 128.309715] x25: ffff0cb9cde93fa0 x24: 0000000000000001<br>[ 128.315969] x23: 0000000000000000 x22: 0000000000000194<br>[ 128.322219] x21: ffff0cd94f986000 x20: 0000000000000000<br>[ 128.328462] x19: ffff0cb9d2a166c0 x18: 0000000000000000<br>[ 128.334698] x17: 0000000000000000 x16: ffffcf1fc523ed24<br>[ 128.340934] x15: 0000ffffd530a518 x14: 0000000000000000<br>[ 128.347162] x13: ffff0cd6bdb31310 x12: 0000000000000368<br>[ 128.353388] x11: ffff0cb9cfbc7070 x10: ffff2cf55dd11e02<br>[ 128.359606] x9 : ffffcf1f85a212b4 x8 : ffff0cd7cf27dab0<br>[ 128.365831] x7 : 0000000000000a20 x6 : ffff0cd7cf27d000<br>[ 128.372040] x5 : 0000000000000000 x4 : 000000000000ffff<br>[ 128.378243] x3 : 0000000000000400 x2 : ffffcf1f85a21294<br>[ 128.384437] x1 : ffff0cb9db520080 x0 : ffff0cb9db500080<br>[ 128.390626] Call trace:<br>[ 128.393964] hclge_ptp_set_tx_info+0x2c/0x140 [hclge]<br>[ 128.399893] hns3_nic_net_xmit+0x39c/0x4c4 [hns3]<br>[ 128.405468] xmit_one.constprop.0+0xc4/0x200<br>[ 128.410600] dev_hard_start_xmit+0x54/0xf0<br>[ 128.415556] sch_direct_xmit+0xe8/0x634<br>[ 128.420246] __dev_queue_xmit+0x224/0xc70<br>[ 128.425101] dev_queue_xmit+0x1c/0x40<br>[ 128.429608] ovs_vport_send+0xac/0x1a0 [openvswitch]<br>[ 128.435409] do_output+0x60/0x17c [openvswitch]<br>[ 128.440770] do_execute_actions+0x898/0x8c4 [openvswitch]<br>[ 128.446993] ovs_execute_actions+0x64/0xf0 [openvswitch]<br>[ 128.453129] ovs_dp_process_packet+0xa0/0x224 [openvswitch]<br>[ 128.459530] ovs_vport_receive+0x7c/0xfc [openvswitch]<br>[ 128.465497] internal_dev_xmit+0x34/0xb0 [openvswitch]<br>[ 128.471460] xmit_one.constprop.0+0xc4/0x200<br>[ 128.476561] dev_hard_start_xmit+0x54/0xf0<br>[ 128.481489] __dev_queue_xmit+0x968/0xc70<br>[ 128.486330] dev_queue_xmit+0x1c/0x40<br>[ 128.490856] ip_finish_output2+0x250/0x570<br>[ 128.495810] __ip_finish_output+0x170/0x1e0<br>[ 128.500832] ip_finish_output+0x3c/0xf0<br>[ 128.505504] ip_output+0xbc/0x160<br>[ 128.509654] ip_send_skb+0x58/0xd4<br>[ 128.513892] udp_send_skb+0x12c/0x354<br>[ 128.518387] udp_sendmsg+0x7a8/0x9c0<br>[ 128.522793] inet_sendmsg+0x4c/0x8c<br>[ 128.527116] __sock_sendmsg+0x48/0x80<br>[ 128.531609] __sys_sendto+0x124/0x164<br>[ 128.536099] __arm64_sys_sendto+0x30/0x5c<br>[ 128.540935] invoke_syscall+0x50/0x130<br>[ 128.545508] el0_svc_common.constprop.0+0x10c/0x124<br>[ 128.551205] do_el0_svc+0x34/0xdc<br>[ 128.555347] el0_svc+0x20/0x30<br>[ 128.559227] el0_sync_handler+0xb8/0xc0<br>[ 128.563883] el0_sync+0x160/0x180 | 2025-01-19 | 5.5 |
| CVE-2024-57914 | linux - multiple products | In the Linux kernel, the following vulnerability has been resolved:<br><br>usb: typec: tcpci: fix NULL pointer issue on shared irq case<br><br>The tcpci_irq() may meet below NULL pointer dereference issue: | 2025-01-19 | 5.5 |

| | | | | |
|---|---|---|---|---|
| | | [ 2.641851] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000010<br>[ 2.641951] status 0x1, 0x37f<br>[ 2.650659] Mem abort info:<br>[ 2.656490] ESR = 0x0000000096000004<br>[ 2.660230] EC = 0x25: DABT (current EL), IL = 32 bits<br>[ 2.665532] SET = 0, FnV = 0<br>[ 2.668579] EA = 0, S1PTW = 0<br>[ 2.671715] FSC = 0x04: level 0 translation fault<br>[ 2.676584] Data abort info:<br>[ 2.679459] ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000<br>[ 2.684936] CM = 0, WnR = 0, TnD = 0, TagAccess = 0<br>[ 2.689980] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0<br>[ 2.695284] [0000000000000010] user address but active_mm is swapper<br>[ 2.701632] Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP<br>[ 2.707883] Modules linked in:<br>[ 2.710936] CPU: 1 UID: 0 PID: 87 Comm: irq/111-2-0051 Not tainted 6.12.0-rc6-06316-g7f63786ad3d1-dirty #4<br>[ 2.720570] Hardware name: NXP i.MX93 11X11 EVK board (DT)<br>[ 2.726040] pstate: 60400009 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--)<br>[ 2.732989] pc : tcpci_irq+0x38/0x318<br>[ 2.736647] lr : _tcpci_irq+0x14/0x20<br>[ 2.740295] sp : ffff80008324bd30<br>[ 2.743597] x29: ffff80008324bd70 x28: ffff800080107894 x27: ffff800082198f70<br>[ 2.750721] x26: ffff0000050e6680 x25: ffff000004d172ac x24: ffff0000050f0000<br>[ 2.757845] x23: ffff000004d17200 x22: 0000000000000001 x21: ffff0000050f0000<br>[ 2.764969] x20: ffff000004d17200 x19: 0000000000000000 x18: 0000000000000001<br>[ 2.772093] x17: 0000000000000000 x16: ffff80008183d8a0 x15: ffff00007fbab040<br>[ 2.779217] x14: ffff00007fb918c0 x13: 0000000000000000 x12: 000000000000017a<br>[ 2.786341] x11: 0000000000000001 x10: 0000000000000a90 x9 : ffff80008324bd00<br>[ 2.793465] x8 : ffff0000050f0af0 x7 : ffff00007fbaa840 x6 : 0000000000000031<br>[ 2.800589] x5 : 000000000000017a x4 : 0000000000000002 x3 : 0000000000000002<br>[ 2.807713] x2 : ffff80008324bd3a x1 : 0000000000000010 x0 : 0000000000000000<br>[ 2.814838] Call trace:<br>[ 2.817273] tcpci_irq+0x38/0x318<br>[ 2.820583] _tcpci_irq+0x14/0x20<br>[ 2.823885] irq_thread_fn+0x2c/0xa8<br>[ 2.827456] irq_thread+0x16c/0x2f4<br>[ 2.830940] kthread+0x110/0x114<br>[ 2.834164] ret_from_fork+0x10/0x20<br>[ 2.837738] Code: f9426420 f9001fe0 d2800000 52800201 (f9400a60)<br><br>This may happen on shared irq case. Such as two Type-C ports share one irq. After the first port finished tcpci_register_port(), it may trigger interrupt. However, if the interrupt comes by chance the 2nd port finishes devm_request_threaded_irq(), the 2nd port interrupt handler will run at first. Then the above issue happens due to tcpci is still a NULL pointer in tcpci_irq() when dereference to regmap.<br><br>devm_request_threaded_irq()<br><-- port1 irq comes<br>disable_irq(client->irq);<br>tcpci_register_port()<br><br>This will restore the logic to the state before commit (77e85107a771 "usb: typec: tcpci: support edge irq").<br><br>However, moving tcpci_register_port() earlier creates a problem when use edge irq because tcpci_init() will be called before devm_request_threaded_irq(). The tcpci_init() writes the ALERT_MASK to the hardware to tell it to start generating interrupts but we're not ready to deal with them yet, then the ALERT events may be missed and ALERT line will not recover to high level forever. To avoid the issue, this will also set ALERT_MASK register after devm_request_threaded_irq() return. | | |
| CVE-2024-57915 | linux - multiple products | In the Linux kernel, the following vulnerability has been resolved:<br><br>usb: gadget: u_serial: Disable ep before setting port to null to fix the crash caused by port being null<br><br>Considering that in some extreme cases, when performing the unbinding operation, gserial_disconnect has cleared gser->ioport, which triggers gadget reconfiguration, and then calls gs_read_complete, resulting in access to a null pointer. Therefore, ep is disabled before gserial_disconnect sets port to null to prevent this from happening.<br><br>Call trace:<br>gs_read_complete+0x58/0x240<br>usb_gadget_giveback_request+0x40/0x160<br>dwc3_remove_requests+0x170/0x484<br>dwc3_ep0_out_start+0xb0/0x1d4<br>__dwc3_gadget_start+0x25c/0x720 | 2025-01-19 | 5.5 |

| | | | | |
|---|---|---|---|---|
| | | kretprobe_trampoline.cfi_jt+0x0/0x8<br>kretprobe_trampoline.cfi_jt+0x0/0x8<br>udc_bind_to_driver+0x1d8/0x300<br>usb_gadget_probe_driver+0xa8/0x1dc<br>gadget_dev_desc_UDC_store+0x13c/0x188<br>configfs_write_iter+0x160/0x1f4<br>vfs_write+0x2d0/0x40c<br>ksys_write+0x7c/0xf0<br>__arm64_sys_write+0x20/0x30<br>invoke_syscall+0x60/0x150<br>el0_svc_common+0x8c/0xf8<br>do_el0_svc+0x28/0xa0<br>el0_svc+0x24/0x84 | | |
| CVE-2024-57927 | linux - multiple products | In the Linux kernel, the following vulnerability has been resolved:<br><br>nfs: Fix oops in nfs_netfs_init_request() when copying to cache<br><br>When netfslib wants to copy some data that has just been read on behalf of nfs, it creates a new write request and calls nfs_netfs_init_request() to initialise it, but with a NULL file pointer. This causes nfs_file_open_context() to oops - however, we don't actually need the nfs context as we're only going to write to the cache.<br><br>Fix this by just returning if we aren't given a file pointer and emit a warning if the request was for something other than copy-to-cache.<br><br>Further, fix nfs_netfs_free_request() so that it doesn't try to free the context if the pointer is NULL. | 2025-01-19 | 5.5 |
| CVE-2024-57933 | linux - multiple products | In the Linux kernel, the following vulnerability has been resolved:<br><br>gve: guard XSK operations on the existence of queues<br><br>This patch predicates the enabling and disabling of XSK pools on the existence of queues. As it stands, if the interface is down, disabling or enabling XSK pools would result in a crash, as the RX queue pointer would be NULL. XSK pool registration will occur as part of the next interface up.<br><br>Similarly, xsk_wakeup needs be guarded against queues disappearing while the function is executing, so a check against the GVE_PRIV_FLAGS_NAPI_ENABLED flag is added to synchronize with the disabling of the bit and the synchronize_net() in gve_turndown. | 2025-01-21 | 5.5 |
| CVE-2024-57938 | linux - multiple products | In the Linux kernel, the following vulnerability has been resolved:<br><br>net/sctp: Prevent autoclose integer overflow in sctp_association_init()<br><br>While by default max_autoclose equals to INT_MAX / HZ, one may set net.sctp.max_autoclose to UINT_MAX. There is code in sctp_association_init() that can consequently trigger overflow. | 2025-01-21 | 5.5 |
| CVE-2024-57940 | linux - multiple products | In the Linux kernel, the following vulnerability has been resolved:<br><br>exfat: fix the infinite loop in exfat_readdir()<br><br>If the file system is corrupted so that a cluster is linked to itself in the cluster chain, and there is an unused directory entry in the cluster, 'dentry' will not be incremented, causing condition 'dentry < max_dentries' unable to prevent an infinite loop.<br><br>This infinite loop causes s_lock not to be released, and other tasks will hang, such as exfat_sync_fs().<br><br>This commit stops traversing the cluster chain when there is unused directory entry in the cluster to avoid this infinite loop. | 2025-01-21 | 5.5 |
| CVE-2024-57944 | linux - multiple products | In the Linux kernel, the following vulnerability has been resolved:<br><br>iio: adc: ti-ads1298: Add NULL check in ads1298_init<br><br>devm_kasprintf() can return a NULL pointer on failure. A check on the return value of such a call in ads1298_init() is missing. Add it. | 2025-01-21 | 5.5 |
| CVE-2025-21658 | linux - multiple products | In the Linux kernel, the following vulnerability has been resolved:<br><br>btrfs: avoid NULL pointer dereference if no valid extent tree<br><br>[BUG]<br>Syzbot reported a crash with the following call trace:<br><br>BTRFS info (device loop0): scrub: started on devid 1<br>BUG: kernel NULL pointer dereference, address: 0000000000000208<br>#PF: supervisor read access in kernel mode | 2025-01-21 | 5.5 |

| | | | | |
|---|---|---|---|---|
| | | #PF: error_code(0x0000) - not-present page<br>PGD 106e70067 P4D 106e70067 PUD 107143067 PMD 0<br>Oops: Oops: 0000 [#1] PREEMPT SMP NOPTI<br>CPU: 1 UID: 0 PID: 689 Comm: repro Kdump: loaded Tainted: G O 6.13.0-rc4-custom+ #206<br>Tainted: [O]=OOT_MODULE<br>Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS unknown 02/02/2022<br>RIP: 0010:find_first_extent_item+0x26/0x1f0 [btrfs]<br>Call Trace:<br><TASK><br>scrub_find_fill_first_stripe+0x13d/0x3b0 [btrfs]<br>scrub_simple_mirror+0x175/0x260 [btrfs]<br>scrub_stripe+0x5d4/0x6c0 [btrfs]<br>scrub_chunk+0xbb/0x170 [btrfs]<br>scrub_enumerate_chunks+0x2f4/0x5f0 [btrfs]<br>btrfs_scrub_dev+0x240/0x600 [btrfs]<br>btrfs_ioctl+0x1dc8/0x2fa0 [btrfs]<br>? do_sys_openat2+0xa5/0xf0<br>__x64_sys_ioctl+0x97/0xc0<br>do_syscall_64+0x4f/0x120<br>entry_SYSCALL_64_after_hwframe+0x76/0x7e<br></TASK><br><br>[CAUSE]<br>The reproducer is using a corrupted image where extent tree root is corrupted, thus forcing to use "rescue=all,ro" mount option to mount the image.<br><br>Then it triggered a scrub, but since scrub relies on extent tree to find where the data/metadata extents are, scrub_find_fill_first_stripe() relies on an non-empty extent root.<br><br>But unfortunately scrub_find_fill_first_stripe() doesn't really expect an NULL pointer for extent root, it use extent_root to grab fs_info and triggered a NULL pointer dereference.<br><br>[FIX]<br>Add an extra check for a valid extent root at the beginning of scrub_find_fill_first_stripe().<br><br>The new error path is introduced by 42437a6386ff ("btrfs: introduce mount option rescue=ignorebadroots"), but that's pretty old, and later commit b979547513ff ("btrfs: scrub: introduce helper to find and fill sector info for a scrub_stripe") changed how we do scrub.<br><br>So for kernels older than 6.6, the fix will need manual backport. | | |
| CVE-2023-40108 | google - Android | In multiple locations, there is a possible way to access media content belonging to another user due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. | 2025-01-21 | 5.5 |
| CVE-2024-49733 | google - Android | In reload of ServiceListing.java , there is a possible way to allow a malicious app to hide an NLS from Settings due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. | 2025-01-21 | 5.5 |
| CVE-2025-0604 | red hat - multiple products | A flaw was found in Keycloak. When an Active Directory user resets their password, the system updates it without performing an LDAP bind to validate the new credentials against AD. This vulnerability allows users whose AD accounts are expired or disabled to regain access in Keycloak, bypassing AD restrictions. The issue enables authentication bypass and could allow unauthorized access under certain conditions. | 2025-01-22 | 5.4 |
| CVE-2025-21262 | microsoft - Microsoft Edge (Chromium-based) | User Interface (UI) Misrepresentation of Critical Information in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network | 2025-01-24 | 5.4 |
| CVE-2024-35112 | ibm - Control Center | IBM Control Center 6.2.1 and 6.3.1<br><br>could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. | 2025-01-25 | 5.4 |
| CVE-2024-22348 | ibm - multiple products | IBM DevOps Velocity 5.0.0 and IBM UrbanCode Velocity 4.0.0 through 4.0. 25 uses Cross-Origin Resource Sharing (CORS) which could allow an attacker to carry out privileged actions and retrieve sensitive information as the domain name is not being limited to only trusted domains. | 2025-01-20 | 5.3 |
| CVE-2025-20128 | cisco - Cisco Secure Endpoint | A vulnerability in the Object Linking and Embedding 2 (OLE2) decryption routine of ClamAV could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device._x000D_<br>_x000D_<br>This vulnerability is due to an integer underflow in a bounds check that allows for a heap buffer overflow read. An attacker could exploit this vulnerability by submitting a crafted file containing OLE2 content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to terminate the ClamAV scanning process, resulting in a DoS condition on the affected software._x000D_<br>For a description of this vulnerability, see the ._x000D_<br>Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. | 2025-01-22 | 5.3 |

| | | | | |
|---|---|---|---|---|
| CVE-2024-40706 | ibm - InfoSphere Information Server | IBM InfoSphere Information Server 11.7 could allow a remote user to obtain sensitive version information that could aid in further attacks against the system. | 2025-01-24 | 5.3 |
| CVE-2023-38012 | ibm - Cloud Pak System | IBM Cloud Pak System 2.3.3.6, 2.3.3.6 iFix1, 2.3.3.6 iFix2, 2.3.3.7, 2.3.3.7 iFix1, and 2.3.4.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. | 2025-01-25 | 5.3 |
| CVE-2023-38013 | ibm - Cloud Pak System | IBM Cloud Pak System 2.3.3.0, 2.3.3.3, 2.3.3.3 iFix1, 2.3.3.4, 2.3.3.5, 2.3.3.6, 2.3.3.6 iFix1, 2.3.3.6 iFix2, 2.3.3.7, and 2.3.3.7 iFix1 could disclose sensitive information in HTTP responses that could aid in further attacks against the system. | 2025-01-25 | 5.3 |
| CVE-2023-38713 | ibm - Cloud Pak System | IBM Cloud Pak System 2.3.3.0, 2.3.3.3, 2.3.3.3 iFix1, 2.3.3.4, 2.3.3.5, 2.3.3.6, 2.3.3.6 iFix1, 2.3.3.6 iFix2, 2.3.3.7, and 2.3.3.7 iFix1 could disclose sensitive information about the system that could aid in further attacks against the system. | 2025-01-25 | 5.3 |
| CVE-2023-38714 | ibm - Cloud Pak System | IBM Cloud Pak System 2.3.3.0, 2.3.3.3, 2.3.3.3 iFix1, 2.3.3.4, 2.3.3.5, 2.3.3.6, 2.3.3.6 iFix1, 2.3.3.6 iFix2, 2.3.3.7, and 2.3.3.7 iFix1 could disclose sensitive information about the system that could aid in further attacks against the system. | 2025-01-25 | 5.3 |
| CVE-2023-38716 | ibm - Cloud Pak System | IBM Cloud Pak System 2.3.3.6, 2.3.36 iFix1, 2.3.3.6 iFix2, 2.3.3.7, 2.3.3.7 iFix1, and 2.3.4.0 could disclose sensitive information about the system that could aid in further attacks against the system. | 2025-01-25 | 5.3 |
| CVE-2024-35114 | ibm - Control Center | IBM Control Center 6.2.1 and 6.3.1<br><br>could allow a remote attacker to enumerate usernames due to an observable discrepancy between login attempts. | 2025-01-25 | 5.3 |
| CVE-2024-35134 | ibm - Analytics Content Hub | IBM Analytics Content Hub 2.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. | 2025-01-25 | 5.3 |
| CVE-2024-35144 | ibm - Maximo Application Suite | IBM Maximo Application Suite 8.10, 8.11, and 9.0 - Monitor Component stores source code on the web server that could aid in further attacks against the system. | 2025-01-25 | 5.3 |
| CVE-2024-35150 | ibm - Maximo Application Suite | IBM Maximo Application Suite 8.10.12, 8.11.0, 9.0.1, and 9.1.0 - Monitor Component does not neutralize output that is written to logs, which could allow an attacker to inject false log entries. | 2025-01-25 | 5.3 |
| CVE-2024-45478 | apache software foundation - Apache Ranger | Stored XSS vulnerability in Edit Service Page of Apache Ranger UI in Apache Ranger Version 2.4.0. Users are recommended to upgrade to version Apache Ranger 2.5.0, which fixes this issue. | 2025-01-21 | 4.8 |
| CVE-2022-23439 | fortinet - multiple products | A externally controlled reference to a resource in another sphere in Fortinet FortiManager before version 7.4.3, FortiMail before version 7.0.3, FortiAnalyzer before version 7.4.3, FortiVoice version 7.0.0, 7.0.1 and before 6.4.8, FortiProxy before version 7.0.4, FortiRecorder version 6.4.0 through 6.4.2 and before 6.0.10, FortiAuthenticator version 6.4.0 through 6.4.1 and before 6.3.3, FortiNDR version 7.2.0 before 7.1.0, FortiWLC before version 8.6.4, FortiPortal before version 6.0.9, FortiOS version 7.2.0 and before 7.0.5, FortiADC version 7.0.0 through 7.0.1 and before 6.2.3 , FortiDDoS before version 5.5.1, FortiDDoS-F before version 6.3.3, FortiTester before version 7.2.1, FortiSOAR before version 7.2.2 and FortiSwitch before version 6.3.3 allows attacker to poison web caches via crafted HTTP requests, where the `Host` header points to an arbitrary webserver | 2025-01-22 | 4.7 |
| CVE-2023-32340 | ibm - Sterling B2B Integrator Standard Edition | IBM Sterling B2B Integrator 6.0.0.0 through 6.1.2.5 and 6.2.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. | 2025-01-23 | 4.6 |
| CVE-2024-51457 | ibm - Robotic Process Automation for Cloud Pak | IBM Robotic Process Automation for Cloud Pak 21.0.0 through 21.0.7.19 and 23.0.0 through 23.0.19 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. | 2025-01-22 | 4.4 |
| CVE-2024-45653 | ibm - Sterling Connect:Direct Web Services | IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 could disclose sensitive IP address information to authenticated users in responses that could be used in further attacks against the system. | 2025-01-19 | 4.3 |
| CVE-2024-45654 | ibm - Security ReaQta | IBM Security ReaQta 3.12 could allow an authenticated user to perform unauthorized actions due to reliance on untrusted inputs. | 2025-01-19 | 4.3 |
| CVE-2023-38271 | ibm - Cloud Pak System | IBM Cloud Pak System 2.3.3.0, 2.3.3.3, 2.3.3.3 iFix1, 2.3.3.4, 2.3.3.5, 2.3.3.6, 2.3.3.6 iFix1, 2.3.3.6 iFix2, 2.3.3.7, and 2.3.3.7 iFix1 could allow an authenticated user to obtain sensitive information from log files. | 2025-01-25 | 4.3 |
| CVE-2024-35111 | ibm - Control Center | IBM Control Center 6.2.1 and 6.3.1 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. | 2025-01-25 | 4.3 |
| CVE-2024-35113 | ibm - Control Center | IBM Control Center 6.2.1 and 6.3.1<br><br>could allow an authenticated user to obtain sensitive information exposed through a directory listing. | 2025-01-25 | 4.3 |
| CVE-2024-13176 | openssl - OpenSSL | Issue summary: A timing side-channel which could potentially allow recovering the private key exists in the ECDSA signature computation.<br><br>Impact summary: A timing side-channel in ECDSA signature computations could allow recovering the private key by an attacker. However, measuring the timing would require either local access to the signing application or a very fast network connection with low latency.<br><br>There is a timing signal of around 300 nanoseconds when the top word of the inverted ECDSA nonce value is zero. This can happen with significant probability only for some of the supported elliptic curves. In particular the NIST P-521 curve is affected. To be able to measure this leak, the attacker | 2025-01-20 | 4.1 |

| | | | | |
|---|---|---|---|---|
| | | process must either be located in the same physical computer or must have a very fast network connection with low latency. For that reason the severity of this vulnerability is Low. | | |
| CVE-2024-22349 | ibm - multiple products | IBM DevOps Velocity 5.0.0 and IBM UrbanCode Velocity 4.0.0 through 4.0. 25 allows web pages to be stored locally which can be read by another user on the system. | 2025-01-20 | 4 |
| CVE-2024-35122 | ibm - i | IBM i 7.2, 7.3, 7.4, and 7.5 is vulnerable to a file level local denial of service caused by an insufficient authority requirement. A local non-privileged user can configure a referential constraint with the privileges of a user socially engineered to access the target file. | 2025-01-24 | 2.8 |

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.