الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

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

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

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 18th of June to 24st of June. 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**

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 18 يونيو إلى 24 يونيو. 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**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2019-25136	mozilla - firefox	A compromised child process could have injected XBL Bindings into privileged CSS rules, resulting in arbitrary code execution and a sandbox escape. This vulnerability affects Firefox < 70.	2023-06-19	10	Critical
CVE-2023-36355	tp-link - tl-wr940n_firmware	TP-Link TL-WR940N V4 was discovered to contain a buffer overflow via the ipStart parameter at /userRpm/WanDynamicIpV6CfgRpm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted GET request.	2023-06-22	9.9	Critical
CVE-2023-29531	mozilla - multiple products	An attacker could have caused an out of bounds memory access using WebGL APIs, leading to memory corruption and a potentially exploitable crash. *This bug only affects Firefox and Thunderbird for macOS. Other operating systems are unaffected.* This vulnerability affects Firefox < 112, Firefox ESR < 102.10, and Thunderbird < 102.10.	2023-06-19	9.8	Critical
CVE-2023-32216	mozilla - firefox	Memory safety bugs present in Firefox 112. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 113.	2023-06-19	9.8	Critical
CVE-2023-25736	mozilla - firefox	An invalid downcast from `nsHTMLDocument` to `nsIContent` could have lead to undefined behavior. This vulnerability affects Firefox < 110.	2023-06-19	9.8	Critical
CVE-2023-29542	mozilla - multiple products	A newline in a filename could have been used to bypass the file extension security mechanisms that replace malicious file extensions such as .lnk with .download. This could have led to accidental execution of malicious code. *This bug only affects Firefox and Thunderbird on Windows. Other versions of Firefox and Thunderbird are unaffected.* This vulnerability affects Firefox < 112, Firefox ESR < 102.10, and Thunderbird < 102.10.	2023-06-19	9.8	Critical
CVE-2023-34416	mozilla - multiple products	Memory safety bugs present in Firefox 113, Firefox ESR 102.11, and Thunderbird 102.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 102.12, Firefox < 114, and Thunderbird < 102.12.	2023-06-19	9.8	Critical
CVE-2023-34417	mozilla - firefox	Memory safety bugs present in Firefox 113. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 114.	2023-06-19	9.8	Critical
CVE-2023-27992	zyxel - nas326_firmware	The pre-authentication command injection vulnerability in the Zyxel NAS326 firmware versions prior to V5.21(AAZF.14)C0, NAS540 firmware versions prior to V5.21(AATB.11)C0, and NAS542 firmware versions prior to V5.21(ABAG.11)C0 could allow an unauthenticated attacker to execute some operating system (OS) commands remotely by sending a crafted HTTP request.	2023-06-19	9.8	Critical

CVE-2023-34159	huawei - emui	Improper permission control vulnerability in the Notepad app.Successful exploitation of the vulnerability may lead to privilege escalation, which affects availability and confidentiality.	2023-06-19	9.8	Critical
CVE-2023-35854	zohocorp - multiple products	Zoho ManageEngine ADSelfService Plus through 6113 has an authentication bypass that can be exploited to steal the domain controller session token for identity spoofing, thereby achieving the privileges of the domain controller administrator.	2023-06-20	9.8	Critical
CVE-2023-34563	netgear - r6250_firmware	netgear R6250 Firmware Version 1.0.4.48 is vulnerable to Buffer Overflow after authentication.	2023-06-20	9.8	Critical
CVE-2023-34340	apache - accumulo	Improper Authentication vulnerability in Apache Software Foundation Apache Accumulo. This issue affects Apache Accumulo: 2.1.0. Accumulo 2.1.0 contains a defect in the user authentication process that may succeed when invalid credentials are provided. Users are advised to upgrade to 2.1.1.	2023-06-21	9.8	Critical
CVE-2023-20892	vmware - multiple products	The vCenter Server contains a heap overflow vulnerability due to the usage of uninitialized memory in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may exploit heap-overflow vulnerability to execute arbitrary code on the underlying operating system that hosts vCenter Server.	2023-06-22	9.8	Critical
CVE-2023-20893	vmware - multiple products	The VMware vCenter Server contains a use-after-free vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may exploit this issue to execute arbitrary code on the underlying operating system that hosts vCenter Server.	2023-06-22	9.8	Critical
CVE-2023-20894	vmware - multiple products	The VMware vCenter Server contains an out-of-bounds write vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger an out-of-bound write by sending a specially crafted packet leading to memory corruption.	2023-06-22	9.8	Critical
CVE-2023-20895	vmware - multiple products	The VMware vCenter Server contains a memory corruption vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger a memory corruption vulnerability which may bypass authentication.	2023-06-22	9.8	Critical
CVE-2023-3128	grafana - multiple products	Grafana is validating Azure AD accounts based on the email claim. On Azure AD, the profile email field is not unique and can be easily modified. This leads to account takeover and authentication bypass when Azure AD OAuth is configured with a multi-tenant app.	2023-06-22	9.8	Critical
CVE-2022-22630	apple - multiple products	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.6.6, macOS Monterey 12.3, Security Update 2022-004 Catalina. A remote user may cause an unexpected app termination or arbitrary code execution	2023-06-23	9.8	Critical
CVE-2023-32387	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.4, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. A remote attacker may be able to cause unexpected app termination or arbitrary code execution	2023-06-23	9.8	Critical
CVE-2023-32412	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in watchOS 9.5, iOS 15.7.6 and iPadOS 15.7.6, macOS Ventura 13.4, tvOS 16.5, iOS 16.5 and iPadOS 16.5, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. A remote attacker may be able to cause unexpected app termination or arbitrary code execution	2023-06-23	9.8	Critical
CVE-2023-32419	apple - multiple products	The issue was addressed with improved bounds checks. This issue is fixed in iOS 16.5 and iPadOS 16.5. A remote attacker may be able to cause arbitrary code execution	2023-06-23	9.8	Critical
CVE-2023-29534	mozilla - multiple products	Different techniques existed to obscure the fullscreen notification in Firefox and Focus for Android. These could have led to potential user confusion and spoofing attacks. *This bug only affects Firefox and Focus for Android. Other versions of Firefox are unaffected.* This vulnerability affects Firefox for Android < 112 and Focus for Android < 112.	2023-06-19	9.1	Critical
CVE-2023-36271	gnu - libredwg	LibreDWG v0.12.5 was discovered to contain a heap buffer overflow via the function bit_wcs2nlen at bits.c.	2023-06-23	8.8	High
CVE-2023-36272	gnu - libredwg	LibreDWG v0.12.5 was discovered to contain a heap buffer overflow via the function bit_utf8_to_TU at bits.c.	2023-06-23	8.8	High
CVE-2023-36273	gnu - libredwg	LibreDWG v0.12.5 was discovered to contain a heap buffer overflow via the function bit_calc_CRC at bits.c.	2023-06-23	8.8	High
CVE-2023-36274	gnu - libredwg	LibreDWG v0.12.5 was discovered to contain a heap buffer overflow via the function bit_write_TF at bits.c.	2023-06-23	8.8	High

CVE-2023-32373	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in watchOS 9.5, iOS 15.7.6 and iPadOS 15.7.6, macOS Ventura 13.4, Safari 16.5, tvOS 16.5, iOS 16.5 and iPadOS 16.5. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.	2023-06-23	8.8	High
CVE-2023-32435	apple - multiple products	A memory corruption issue was addressed with improved state management. This issue is fixed in Safari 16.4, iOS 16.4 and iPadOS 16.4, macOS Ventura 13.3, iOS 15.7.7 and iPadOS 15.7.7. Processing web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited against versions of iOS released before iOS 15.7.	2023-06-23	8.8	High
CVE-2023-32439	apple - multiple products	A type confusion issue was addressed with improved checks. This issue is fixed in iOS 16.5.1 and iPadOS 16.5.1, Safari 16.5.1, macOS Ventura 13.4.1, iOS 15.7.7 and iPadOS 15.7.7. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.	2023-06-23	8.8	High
CVE-2023-32409	apple - multiple products	The issue was addressed with improved bounds checks. This issue is fixed in watchOS 9.5, macOS Ventura 13.4, Safari 16.5, tvOS 16.5, iOS 16.5 and iPadOS 16.5. A remote attacker may be able to break out of Web Content sandbox. Apple is aware of a report that this issue may have been actively exploited.	2023-06-23	8.6	High
CVE-2023-32414	apple - macos	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.4. An app may be able to break out of its sandbox	2023-06-23	8.6	High
CVE-2023-28956	ibm - spectrum_protect_backup-archive_client	IBM Spectrum Protect Backup-Archive Client 8.1.0.0 through 8.1.17.2 may allow a local user to escalate their privileges due to improper access controls. IBM X-Force ID: 251767.	2023-06-22	7.8	High
CVE-2023-32449	dell - powerstoret_os	Dell PowerStore versions prior to 3.5 contain an improper verification of cryptographic signature vulnerability. An attacker can trick a high privileged user to install a malicious binary by bypassing the existing cryptographic signature checks	2023-06-22	7.8	High
CVE-2023-28073	dell - precision_3570_firmware	Dell BIOS contains an improper authentication vulnerability. A locally authenticated malicious user may potentially exploit this vulnerability by bypassing certain authentication mechanisms in order to elevate privileges on the system.	2023-06-23	7.8	High
CVE-2023-23516	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6.3, macOS Big Sur 11.7.3, macOS Ventura 13.2. An app may be able to execute arbitrary code with kernel privileges	2023-06-23	7.8	High
CVE-2023-23539	apple - macos	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2. Mounting a maliciously crafted Samba network share may lead to arbitrary code execution	2023-06-23	7.8	High
CVE-2023-27930	apple - multiple products	A type confusion issue was addressed with improved checks. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4, watchOS 9.5, tvOS 16.5. An app may be able to execute arbitrary code with kernel privileges	2023-06-23	7.8	High
CVE-2023-32351	apple - itunes	A logic issue was addressed with improved checks. This issue is fixed in iTunes 12.12.9 for Windows. An app may be able to gain elevated privileges	2023-06-23	7.8	High
CVE-2023-32353	apple - itunes	A logic issue was addressed with improved checks. This issue is fixed in iTunes 12.12.9 for Windows. An app may be able to elevate privileges	2023-06-23	7.8	High
CVE-2023-32380	apple - multiple products	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.4, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. Processing a 3D model may lead to arbitrary code execution	2023-06-23	7.8	High
CVE-2023-32384	apple - multiple products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in watchOS 9.5, iOS 15.7.6 and iPadOS 15.7.6, macOS Ventura 13.4, tvOS 16.5, iOS 16.5 and iPadOS 16.5, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. Processing an image may lead to arbitrary code execution	2023-06-23	7.8	High
CVE-2023-32398	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in watchOS 9.5, iOS 15.7.6 and iPadOS 15.7.6, macOS Ventura 13.4, tvOS 16.5, iOS 16.5 and iPadOS 16.5, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. An app may be able to execute arbitrary code with kernel privileges	2023-06-23	7.8	High
CVE-2023-32405	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.4, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. An app may be able to gain root privileges	2023-06-23	7.8	High
CVE-2023-32434	apple - multiple products	An integer overflow was addressed with improved input validation. This issue is fixed in watchOS 8.8.1, iOS 16.5.1 and iPadOS 16.5.1, iOS 15.7.7 and iPadOS 15.7.7, macOS Big Sur 11.7.8, macOS Monterey 12.6.7, macOS Ventura 13.4.1, watchOS 9.5.2. An app may be able to execute arbitrary code with kernel	2023-06-23	7.8	High

		privileges. Apple is aware of a report that this issue may have been actively exploited against versions of iOS released before iOS 15.7.			
CVE-2023-36356	tp-link - tl-wr940n_firmware	TP-Link TL-WR940N V2/V4/V6, TL-WR841N V8, TL-WR941ND V5, and TL-WR740N V1/V2 were discovered to contain a buffer read out-of-bounds via the component /userRpm/VirtualServerRpm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted GET request.	2023-06-22	7.7	High
CVE-2023-36357	tp-link - tl-wr940n_firmware	An issue in the /userRpm/LocalManageControlRpm component of TP-Link TL-WR940N V2/V4/V6, TL-WR841N V8/V10, and TL-WR941ND V5 allows attackers to cause a Denial of Service (DoS) via a crafted GET request.	2023-06-22	7.7	High
CVE-2023-36358	tp-link - tl-wr940n_firmware	TP-Link TL-WR940N V2/V3/V4, TL-WR941ND V5/V6, TL-WR743ND V1 and TL-WR841N V8 were discovered to contain a buffer overflow in the component /userRpm/AccessCtrlAccessTargetsRpm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted GET request.	2023-06-22	7.7	High
CVE-2023-32209	mozilla - firefox	A maliciously crafted favicon could have led to an out of memory crash. This vulnerability affects Firefox < 113.	2023-06-19	7.5	High
CVE-2023-32214	mozilla - multiple products	Protocol handlers \`ms-cxh\` and \`ms-cxh-full\` could have been leveraged to trigger a denial of service. *Note: This attack only affects Windows. Other operating systems are not affected.* This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11.	2023-06-19	7.5	High
CVE-2023-25733	mozilla - firefox	The return value from \`gfx::SourceSurfaceSkia::Map()\` wasn't being verified which could have potentially lead to a null pointer dereference. This vulnerability affects Firefox < 110.	2023-06-19	7.5	High
CVE-2023-25747	mozilla - firefox	A potential use-after-free in libaudio was fixed by disabling the AAudio backend when running on Android API below version 30. *This bug only affects Firefox for Android. Other versions of Firefox are unaffected.* This vulnerability affects Firefox for Android < 110.1.0.	2023-06-19	7.5	High
CVE-2022-48486	huawei - emui	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	2023-06-19	7.5	High
CVE-2022-48487	huawei - emui	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	2023-06-19	7.5	High
CVE-2022-48489	huawei - emui	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	2023-06-19	7.5	High
CVE-2022-48490	huawei - emui	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	2023-06-19	7.5	High
CVE-2022-48492	huawei - emui	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	2023-06-19	7.5	High
CVE-2022-48493	huawei - emui	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	2023-06-19	7.5	High
CVE-2022-48494	huawei - multiple products	Vulnerability of lax app identity verification in the pre-authorization function.Successful exploitation of this vulnerability will cause malicious apps to become pre-authorized.	2023-06-19	7.5	High
CVE-2022-48496	huawei - multiple products	Vulnerability of lax app identity verification in the pre-authorization function.Successful exploitation of this vulnerability will cause malicious apps to become pre-authorized.	2023-06-19	7.5	High
CVE-2022-48497	huawei - emui	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	2023-06-19	7.5	High
CVE-2022-48498	huawei - emui	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	2023-06-19	7.5	High
CVE-2022-48499	huawei - emui	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	2023-06-19	7.5	High
CVE-2022-48500	huawei - emui	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	2023-06-19	7.5	High
CVE-2022-48501	huawei - emui	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	2023-06-19	7.5	High
CVE-2023-34155	huawei - emui	Vulnerability of unauthorized calling on HUAWEI phones and tablets.Successful exploitation of this vulnerability may affect availability.	2023-06-19	7.5	High
CVE-2023-34161	huawei - multiple products	nappropriate authorization vulnerability in the SettingsProvider module.Successful exploitation of this vulnerability may cause features to perform abnormally.	2023-06-19	7.5	High
CVE-2023-34162	huawei - emui	Version update determination vulnerability in the user profile module.Successful exploitation of this vulnerability may cause repeated HMS Core updates and cause services to fail.	2023-06-19	7.5	High
CVE-2023-34163	huawei - multiple products	Permission control vulnerability in the window management module.Successful exploitation of this vulnerability may cause features to perform abnormally.	2023-06-19	7.5	High
CVE-2023-34166	huawei - multiple products	Vulnerability of system restart triggered by abnormal callbacks passed to APIs.Successful exploitation of this vulnerability may cause the system to restart.	2023-06-19	7.5	High
CVE-2023-3312	linux - linux_kernel	A vulnerability was found in drivers/cpufreq/qcom-cpufreq-hw.c in cpufreq subsystem in the Linux Kernel. This flaw, during device unbind will lead to double release problem leading to denial of service.	2023-06-19	7.5	High

CVE-2023-34981	apache - multiple products	A regression in the fix for bug 66512 in Apache Tomcat 11.0.0-M5, 10.1.8, 9.0.74 and 8.5.88 meant that, if a response did not include any HTTP headers no AJP SEND_HEADERS messare woudl be sent for the response which in turn meant that at least one AJP proxy (mod_proxy_ajp) would use the response headers from the previous request leading to an information leak.	2023-06-21	7.5	High
CVE-2023-0026	juniper - multiple products	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When a BGP update message is received over an established BGP session, and that message contains a specific, optional transitive attribute, this session will be torn down with an update message error. This issue cannot propagate beyond an affected system as the processing error occurs as soon as the update is received. This issue is exploitable remotely as the respective attribute can propagate through unaffected systems and intermediate AS (if any). Continuous receipt of a BGP update containing this attribute will create a sustained Denial of Service (DoS) condition. Some customers have experienced these BGP session flaps which prompted Juniper SIRT to release this advisory out of cycle before fixed releases are widely available as there is an effective workaround. This issue affects: Juniper Networks Junos OS 15.1R1 and later versions prior to 20.4R3-S8; 21.1 version 21.1R1 and later versions prior to 21.2R3-S6; 21.3 versions prior to 21.3R3-S5; 21.4 versions prior to 21.4R3-S4; 22.1 versions prior to 22.1R3-S4; 22.2 versions prior to 22.2R3-S2; 22.3 versions prior to 22.2R3-S2; 22.4 versions prior to 22.4R2-S1, 22.4R3; 23.1 versions prior to 23.1R1-S1, 23.1R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S8-EVO; 21.1 version 21.1R1-EVO and later versions prior to 21.2R3-S6-EVO; 21.3 versions prior to 21.3R3-S5-EVO; 21.4 versions prior to 21.4R3-S4-EVO; 22.1 versions prior to 22.1R3-S4-EVO; 22.2 versions prior to 22.2R3-S2-EVO; 22.3 versions prior to 22.3R2-S2-EVO, 22.3R3-S1-EVO; 22.4 versions prior to 22.4R2-S1-EVO, 22.4R3-EVO; 23.1 versions prior to 23.1R1-S1-EVO, 23.1R2-EVO.	2023-06-21	7.5	High
CVE-2023-20896	vmware - multiple products	The VMware vCenter Server contains an out-of-bounds read vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger an out-of-bounds read by sending a specially crafted packet leading to denial-of-service of certain services (vmcad, vmdird, and vmafdd).	2023-06-22	7.5	High
CVE-2023-36354	tp-link - tl-wr940n_firmware	TP-Link TL-WR940N V4, TL-WR841N V8/V10, TL-WR740N V1/V2, TL-WR940N V2/V3, and TL-WR941ND V5/V6 were discovered to contain a buffer overflow in the component /userRpm/AccessCtrlTimeSchedRpm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted GET request.	2023-06-22	7.5	High
CVE-2023-36359	tp-link - tl-wr940n_firmware	TP-Link TL-WR940N V4, TL-WR841N V8/V10, TL-WR940N V2/V3 and TL-WR941ND V5/V6 were discovered to contain a buffer overflow in the component /userRpm/QoSRuleListRpm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted GET request.	2023-06-22	7.5	High
CVE-2023-33141	microsoft - multiple products	Yet Another Reverse Proxy (YARP) Denial of Service Vulnerability	2023-06-23	7.5	High
CVE-2023-32397	apple - multiple products	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.4, macOS Big Sur 11.7.7, iOS 15.7.6 and iPadOS 15.7.6, macOS Monterey 12.6.6. An app may be able to modify protected parts of the file system	2023-06-23	7.5	High
CVE-2023-28065	dell - multiple products	Dell Command | Update, Dell Update, and Alienware Update versions 4.8.0 and prior contain an Insecure Operation on Windows Junction / Mount Point vulnerability. A local malicious user could potentially exploit this vulnerability leading to privilege escalation.	2023-06-23	7.3	High
CVE-2023-28071	dell - multiple products	Dell Command | Update, Dell Update, and Alienware Update versions 4.9.0, A01 and prior contain an Insecure Operation on Windows Junction / Mount Point vulnerability. A local malicious user could potentially exploit this vulnerability to create arbitrary folder leading to permanent Denial of Service (DOS).	2023-06-23	7.1	High
CVE-2023-32357	apple - multiple products	An authorization issue was addressed with improved state management. This issue is fixed in watchOS 9.5, macOS Ventura 13.4, tvOS 16.5, iOS 16.5 and iPadOS 16.5, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. An app may be able to retain access to system configuration files even after its permission is revoked	2023-06-23	7.1	High
CVE-2023-32420	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4, watchOS 9.5, tvOS 16.5. An app may be able to cause unexpected system termination or read kernel memory	2023-06-23	7.1	High

CVE-2023-35823	linux - linux_kernel	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in saa7134_finidev in drivers/media/pci/saa7134/saa7134-core.c.	2023-06-18	7	High
CVE-2023-35824	linux - linux_kernel	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in dm1105_remove in drivers/media/pci/dm1105/dm1105.c.	2023-06-18	7	High
CVE-2023-35826	linux - linux_kernel	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in cedrus_remove in drivers/staging/media/sunxi/cedrus/cedrus.c.	2023-06-18	7	High
CVE-2023-35827	linux - linux_kernel	An issue was discovered in the Linux kernel through 6.3.8. A use-after-free was found in ravb_remove in drivers/net/ethernet/renesas/ravb_main.c.	2023-06-18	7	High
CVE-2023-35828	linux - linux_kernel	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in renesas_usb3_remove in drivers/usb/gadget/udc/renesas_usb3.c.	2023-06-18	7	High
CVE-2023-35829	linux - linux_kernel	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in rkvdec_remove in drivers/staging/media/rkvdec/rkvdec.c.	2023-06-18	7	High
CVE-2023-32413	apple - multiple products	A race condition was addressed with improved state handling. This issue is fixed in watchOS 9.5, iOS 15.7.6 and iPadOS 15.7.6, macOS Ventura 13.4, tvOS 16.5, iOS 16.5 and iPadOS 16.5, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. An app may be able to gain root privileges	2023-06-23	7	High
CVE-2023-32480	dell - alienware_m15_r7_firmware	Dell BIOS contains an Improper Input Validation vulnerability. An unauthenticated physical attacker may potentially exploit this vulnerability to perform arbitrary code execution.	2023-06-23	6.8	Medium
CVE-2023-25936	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-25937	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28028	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28029	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable	2023-06-23	6.7	Medium
CVE-2023-28030	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28032	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28033	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28035	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28039	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28040	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium

CVE-2023-28041	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28042	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28052	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28054	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28056	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28059	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28061	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-25938	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28026	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28027	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28031	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28034	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28036	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28044	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28050	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-28058	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges	2023-06-23	6.7	Medium

		may potentially exploit this vulnerability in order to modify a UEFI variable.			
CVE-2023-28060	dell - alienware_area_51m_r1_firmware	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability in order to modify a UEFI variable.	2023-06-23	6.7	Medium
CVE-2023-35005	apache - airflow	In Apache Airflow, some potentially sensitive values were being shown to the user in certain situations. This vulnerability is mitigated by the fact configuration is not shown in the UI by default (only if `[webserver] expose_config` is set to `non-sensitive-only`), and not all uncensored values are actually sentitive. This issue affects Apache Airflow: from 2.5.0 before 2.6.2. Users are recommended to update to version 2.6.2 or later.	2023-06-19	6.5	Medium
CVE-2023-32210	mozilla - firefox	Documents were incorrectly assuming an ordering of principal objects when ensuring we were loading an appropriately privileged principal. In certain circumstances it might have been possible to cause a document to be loaded with a higher privileged principal than intended. This vulnerability affects Firefox < 113.	2023-06-19	6.5	Medium
CVE-2023-29545	mozilla - multiple products	Similar to CVE-2023-28163, this time when choosing 'Save Link As', suggested filenames containing environment variable names would have resolved those in the context of the current user. *This bug only affects Firefox and Thunderbird on Windows. Other versions of Firefox and Thunderbird are unaffected.* This vulnerability affects Firefox < 112, Firefox ESR < 102.10, and Thunderbird < 102.10.	2023-06-19	6.5	Medium
CVE-2023-29546	mozilla - multiple products	When recording the screen while in Private Browsing on Firefox for Android the address bar and keyboard were not hidden, potentially leaking sensitive information. *This bug only affects Firefox for Android. Other operating systems are unaffected.* This vulnerability affects Firefox for Android < 112 and Focus for Android < 112.	2023-06-19	6.5	Medium
CVE-2023-28204	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 9.5, iOS 15.7.6 and iPadOS 15.7.6, macOS Ventura 13.4, Safari 16.5, tvOS 16.5, iOS 16.5 and iPadOS 16.5. Processing web content may disclose sensitive information. Apple is aware of a report that this issue may have been actively exploited.	2023-06-23	6.5	Medium
CVE-2023-32402	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 9.5, macOS Ventura 13.4, Safari 16.5, tvOS 16.5, iOS 16.5 and iPadOS 16.5. Processing web content may disclose sensitive information	2023-06-23	6.5	Medium
CVE-2023-32423	apple - multiple products	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in watchOS 9.5, macOS Ventura 13.4, Safari 16.5, tvOS 16.5, iOS 16.5 and iPadOS 16.5. Processing web content may disclose sensitive information	2023-06-23	6.5	Medium
CVE-2023-27940	apple - multiple products	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.4, iOS 15.7.6 and iPadOS 15.7.6, macOS Monterey 12.6.6. A sandboxed app may be able to observe system-wide network connections	2023-06-23	6.3	Medium
CVE-2023-32371	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4. An app may be able to break out of its sandbox	2023-06-23	6.3	Medium
CVE-2023-34415	mozilla - firefox	When choosing a site-isolated process for a document loaded from a data: URL that was the result of a redirect, Firefox would load that document in the same process as the site that issued the redirect. This bypassed the site-isolation protections against Spectre-like attacks on sites that host an "open redirect". Firefox no longer follows HTTP redirects to data: URLs. This vulnerability affects Firefox < 114.	2023-06-19	6.1	Medium
CVE-2023-32369	apple - multiple products	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.4, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. An app may be able to modify protected parts of the file system	2023-06-23	6	Medium
CVE-2023-29532	mozilla - multiple products	A local attacker can trick the Mozilla Maintenance Service into applying an unsigned update file by pointing the service at an update file on a malicious SMB server. The update file can be replaced after the signature check, before the use, because the write-lock requested by the service does not work on a SMB server. *Note: This attack requires local system access and only affects Windows. Other operating systems are not affected.* This	2023-06-19	5.5	Medium

		vulnerability affects Firefox < 112, Firefox ESR < 102.10, and Thunderbird < 102.10.			
CVE-2023-3022	linux - linux_kernel	A flaw was found in the IPv6 module of the Linux kernel. The arg.result was not used consistently in fib6_rule_lookup, sometimes holding rt6_info and other times fib6_info. This was not accounted for in other parts of the code where rt6_info was expected unconditionally, potentially leading to a kernel panic in fib6_rule_suppress.	2023-06-19	5.5	Medium
CVE-2023-3220	linux - linux_kernel	An issue was discovered in the Linux kernel through 6.1-rc8. dpu_crtc_atomic_check in drivers/gpu/drm/msm/disp/dpu1/dpu_crtc.c lacks check of the return value of kzalloc() and will cause the NULL Pointer Dereference.	2023-06-20	5.5	Medium
CVE-2023-33842	ibm - multiple products	IBM SPSS Modeler on Windows 17.0, 18.0, 18.2.2, 18.3, 18.4, and 18.5 requires the end user to have access to the server SSL key which could allow a local user to decrypt and obtain sensitive information. IBM X-Force ID: 256117.	2023-06-22	5.5	Medium
CVE-2022-42792	apple - multiple products	This issue was addressed with improved data protection. This issue is fixed in iOS 16.1 and iPadOS 16. An app may be able to read sensitive location information	2023-06-23	5.5	Medium
CVE-2022-42860	apple - multiple products	This issue was addressed with improved checks to prevent unauthorized actions. This issue is fixed in macOS Monterey 12.6.1, macOS Big Sur 11.7.1, macOS Ventura 13. An app may be able to modify protected parts of the file system	2023-06-23	5.5	Medium
CVE-2022-46715	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in iOS 16.1 and iPadOS 16. An app may be able to bypass certain Privacy preferences	2023-06-23	5.5	Medium
CVE-2022-46718	apple - multiple products	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 15.7.2 and iPadOS 15.7.2, macOS Ventura 13.1, macOS Big Sur 11.7.2, macOS Monterey 12.6.2. An app may be able to read sensitive location information	2023-06-23	5.5	Medium
CVE-2023-28191	apple - multiple products	This issue was addressed with improved redaction of sensitive information. This issue is fixed in watchOS 9.5, macOS Ventura 13.4, tvOS 16.5, iOS 16.5 and iPadOS 16.5, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. An app may be able to bypass Privacy preferences	2023-06-23	5.5	Medium
CVE-2023-28202	apple - multiple products	This issue was addressed with improved state management. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4, watchOS 9.5, tvOS 16.5. An app firewall setting may not take effect after exiting the Settings app	2023-06-23	5.5	Medium
CVE-2023-32352	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in watchOS 9.5, macOS Ventura 13.4, iOS 16.5 and iPadOS 16.5, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. An app may bypass Gatekeeper checks	2023-06-23	5.5	Medium
CVE-2023-32354	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 16.5 and iPadOS 16.5, watchOS 9.5, tvOS 16.5. An app may be able to disclose kernel memory	2023-06-23	5.5	Medium
CVE-2023-32355	apple - multiple products	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.4, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. An app may be able to modify protected parts of the file system	2023-06-23	5.5	Medium
CVE-2023-32360	apple - multiple products	An authentication issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.4, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. An unauthenticated user may be able to access recently printed documents	2023-06-23	5.5	Medium
CVE-2023-32363	apple - macos	A permissions issue was addressed by removing vulnerable code and adding additional checks. This issue is fixed in macOS Ventura 13.4. An app may be able to bypass Privacy preferences	2023-06-23	5.5	Medium
CVE-2023-32367	apple - multiple products	This issue was addressed with improved entitlements. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4. An app may be able to access user-sensitive data	2023-06-23	5.5	Medium
CVE-2023-32368	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 9.5, macOS Ventura 13.4, tvOS 16.5, iOS 16.5 and iPadOS 16.5, macOS Monterey 12.6.6. Processing a 3D model may result in disclosure of process memory	2023-06-23	5.5	Medium
CVE-2023-32372	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4, watchOS 9.5, tvOS 16.5. Processing an image may result in disclosure of process memory	2023-06-23	5.5	Medium
CVE-2023-32375	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.4, macOS Monterey 12.6.6. Processing a 3D model may result in disclosure of process memory	2023-06-23	5.5	Medium
CVE-2023-32376	apple - multiple products	This issue was addressed with improved entitlements. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4, watchOS 9.5, tvOS 16.5. An app may be able to modify protected parts of the file system	2023-06-23	5.5	Medium
CVE-2023-32382	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.4, macOS Big	2023-06-23	5.5	Medium

		Sur 11.7.7, macOS Monterey 12.6.6. Processing a 3D model may result in disclosure of process memory			
CVE-2023-32385	apple - multiple products	A denial-of-service issue was addressed with improved memory handling. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4. Opening a PDF file may lead to unexpected app termination	2023-06-23	5.5	Medium
CVE-2023-32388	apple - multiple products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in watchOS 9.5, iOS 15.7.6 and iPadOS 15.7.6, macOS Ventura 13.4, iOS 16.5 and iPadOS 16.5, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. An app may be able to bypass Privacy preferences	2023-06-23	5.5	Medium
CVE-2023-32389	apple - multiple products	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4, watchOS 9.5, tvOS 16.5. An app may be able to disclose kernel memory	2023-06-23	5.5	Medium
CVE-2023-32392	apple - multiple products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in watchOS 9.5, macOS Ventura 13.4, tvOS 16.5, iOS 16.5 and iPadOS 16.5, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. An app may be able to read sensitive location information	2023-06-23	5.5	Medium
CVE-2023-32395	apple - multiple products	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.4, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. An app may be able to modify protected parts of the file system	2023-06-23	5.5	Medium
CVE-2023-32399	apple - multiple products	The issue was addressed with improved handling of caches. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4, watchOS 9.5, tvOS 16.5. An app may be able to read sensitive location information	2023-06-23	5.5	Medium
CVE-2023-32400	apple - multiple products	This issue was addressed with improved checks. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4, watchOS 9.5. Entitlements and privacy permissions granted to this app may be used by a malicious app	2023-06-23	5.5	Medium
CVE-2023-32403	apple - multiple products	This issue was addressed with improved redaction of sensitive information. This issue is fixed in watchOS 9.5, iOS 15.7.6 and iPadOS 15.7.6, macOS Ventura 13.4, tvOS 16.5, iOS 16.5 and iPadOS 16.5, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. An app may be able to read sensitive location information	2023-06-23	5.5	Medium
CVE-2023-32404	apple - multiple products	This issue was addressed with improved entitlements. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4, watchOS 9.5. An app may be able to bypass Privacy preferences	2023-06-23	5.5	Medium
CVE-2023-32407	apple - multiple products	A logic issue was addressed with improved state management. This issue is fixed in watchOS 9.5, iOS 15.7.6 and iPadOS 15.7.6, macOS Ventura 13.4, tvOS 16.5, iOS 16.5 and iPadOS 16.5, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. An app may be able to bypass Privacy preferences	2023-06-23	5.5	Medium
CVE-2023-32408	apple - multiple products	The issue was addressed with improved handling of caches. This issue is fixed in watchOS 9.5, iOS 15.7.6 and iPadOS 15.7.6, macOS Ventura 13.4, tvOS 16.5, iOS 16.5 and iPadOS 16.5, macOS Monterey 12.6.6. An app may be able to read sensitive location information	2023-06-23	5.5	Medium
CVE-2023-32410	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.4, macOS Big Sur 11.7.7, iOS 15.7.6 and iPadOS 15.7.6, macOS Monterey 12.6.6. An app may be able to leak sensitive kernel state	2023-06-23	5.5	Medium
CVE-2023-32411	apple - multiple products	This issue was addressed with improved entitlements. This issue is fixed in macOS Ventura 13.4, tvOS 16.5, iOS 16.5 and iPadOS 16.5, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. An app may be able to bypass Privacy preferences	2023-06-23	5.5	Medium
CVE-2023-32415	apple - multiple products	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4, tvOS 16.5. An app may be able to read sensitive location information	2023-06-23	5.5	Medium
CVE-2023-32422	apple - multiple products	This issue was addressed by adding additional SQLite logging restrictions. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4, tvOS 16.5. An app may be able to bypass Privacy preferences	2023-06-23	5.5	Medium
CVE-2023-27964	apple - airpods_firmware	An authentication issue was addressed with improved state management. This issue is fixed in AirPods Firmware Update 5E133. When your headphones are seeking a connection request to one of your previously paired devices, an attacker in Bluetooth range might be able to spoof the intended source device and gain access to your headphones.	2023-06-23	5.4	Medium
CVE-2023-32208	mozilla - firefox	Service workers could reveal script base URL due to dynamic \`import()\`. This vulnerability affects Firefox < 113.	2023-06-19	5.3	Medium
CVE-2022-48488	huawei - multiple products	Vulnerability of bypassing the default desktop security controls.Successful exploitation of this vulnerability may cause unauthorized modifications to the desktop.	2023-06-19	5.3	Medium

CVE-2022-48491	huawei - multiple products	Vulnerability of missing authentication on certain HUAWEI phones.Successful exploitation of this vulnerability can lead to ads and other windows to display at any time.	2023-06-19	5.3	Medium
CVE-2022-48495	huawei - multiple products	Vulnerability of unauthorized access to foreground app information.Successful exploitation of this vulnerability may cause foreground app information to be obtained.	2023-06-19	5.3	Medium
CVE-2023-34156	huawei - multiple products	Vulnerability of services denied by early fingerprint APIs on HarmonyOS products.Successful exploitation of this vulnerability may cause services to be denied.	2023-06-19	5.3	Medium
CVE-2023-34158	huawei - multiple products	Vulnerability of spoofing trustlists of Huawei desktop.Successful exploitation of this vulnerability can cause third-party apps to hide app icons on the desktop to prevent them from being uninstalled.	2023-06-19	5.3	Medium
CVE-2023-34160	huawei - multiple products	Vulnerability of spoofing trustlists of Huawei desktop.Successful exploitation of this vulnerability can cause third-party apps to hide app icons on the desktop to prevent them from being uninstalled.	2023-06-19	5.3	Medium
CVE-2023-34167	huawei - multiple products	Vulnerability of spoofing trustlists of Huawei desktop.Successful exploitation of this vulnerability can cause third-party apps to hide app icons on the desktop to prevent them from being uninstalled.	2023-06-19	5.3	Medium
CVE-2023-28064	dell - alienware_m15_r6_firmware	Dell BIOS contains an Out-of-bounds Write vulnerability. An unauthenticated physical attacker may potentially exploit this vulnerability, leading to denial of service.	2023-06-23	4.6	Medium
CVE-2023-32391	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4, watchOS 9.5, iOS 15.7.6 and iPadOS 15.7.6. A shortcut may be able to use sensitive data with certain actions without prompting the user	2023-06-23	4.6	Medium
CVE-2023-3315	jenkins - team_concert	Missing permission checks in Jenkins Team Concert Plugin 2.4.1 and earlier allow attackers with Overall/Read permission to check for the existence of an attacker-specified file path on the Jenkins controller file system.	2023-06-19	4.3	Medium
CVE-2022-42807	apple - macos	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13. A user may accidentally add a participant to a Shared Album by pressing the Delete key	2023-06-23	4.3	Medium
CVE-2022-42834	apple - multiple products	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Monterey 12.6.3, macOS Ventura 13, macOS Big Sur 11.7.3. An app may be able to access mail folder attachments through a temporary directory used during compression	2023-06-23	3.3	Low
CVE-2023-32386	apple - multiple products	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Ventura 13.4, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. An app may be able to observe unprotected user data	2023-06-23	3.3	Low
CVE-2023-34414	mozilla - multiple products	The error page for sites with invalid TLS certificates was missing the activation-delay Firefox uses to protect prompts and permission dialogs from attacks that exploit human response time delays. If a malicious page elicited user clicks in precise locations immediately before navigating to a site with a certificate error and made the renderer extremely busy at the same time, it could create a gap between when the error page was loaded and when the display actually refreshed. With the right timing the elicited clicks could land in that gap and activate the button that overrides the certificate error for that site. This vulnerability affects Firefox ESR < 102.12, Firefox < 114, and Thunderbird < 102.12.	2023-06-19	3.1	Low
CVE-2023-32365	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 16.5 and iPadOS 16.5, iOS 15.7.6 and iPadOS 15.7.6. Shake-to-undo may allow a deleted photo to be re-surfaced without authentication	2023-06-23	2.4	Low
CVE-2023-32394	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4, watchOS 9.5, tvOS 16.5. A person with physical access to a device may be able to view contact information from the lock screen	2023-06-23	2.4	Low
CVE-2023-32417	apple - watchos	This issue was addressed by restricting options offered on a locked device. This issue is fixed in watchOS 9.5. An attacker with physical access to a locked Apple Watch may be able to view user photos or contacts via accessibility features	2023-06-23	2.4	Low
CVE-2023-32390	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4, watchOS 9.5. Photos belonging to the Hidden Photos Album could be viewed without authentication through Visual Lookup	2023-06-23	2.1	Low

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.