الهيئة الوطنية للأمن السيبراني
Nat onal 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 29th of September to 6th of October. 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 29 سبتمبر إلى 6 أكتوبر. 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-2024-9392	mozilla - multiple products	A compromised content process could have allowed for the arbitrary loading of cross-origin pages. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131.	2024-10-01	9.8	Critical
CVE-2024-9401	mozilla - multiple products	Memory safety bugs present in Firefox 130, Firefox ESR 115.15, Firefox ESR 128.2, and Thunderbird 128.2. 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 < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131.	2024-10-01	9.8	Critical
CVE-2024-9402	mozilla - multiple products	Memory safety bugs present in Firefox 130, Firefox ESR 128.2, and Thunderbird 128.2. 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 < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131.	2024-10-01	9.8	Critical
CVE-2024-44097	google - Android	According to the researcher: "The TLS connections are encrypted against tampering or eavesdropping. However, the application does not validate the server certificate properly while initializing the TLS connection. This allows for a network attacker to intercept the connection and read the data. The attacker could the either send the client a malicious response, or forward the (possibly modified) data to the real server."	2024-10-02	9.8	Critical
CVE-2024-45519	zimbra - multiple products	The postjournal service in Zimbra Collaboration (ZCS) before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1 sometimes allows unauthenticated users to execute commands.	2024-10-02	9.8	Critical
CVE-2024-41593	draytek - vigor3912_firmware	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow.	2024-10-03	9.8	Critical
CVE-2024-20518	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	2024-10-02	9.1	Critical
CVE-2024-20519	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an	2024-10-02	9.1	Critical

		affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.			
CVE-2024-20520	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	2024-10-02	9.1	Critical
CVE-2024-20521	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	2024-10-02	9.1	Critical
CVE-2024-9396	mozilla - multiple products	It is currently unknown if this issue is exploitable but a condition may arise where the structured clone of certain objects could lead to memory corruption. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131.	2024-10-01	8.8	High
CVE-2024-9400	mozilla - multiple products	A potential memory corruption vulnerability could be triggered if an attacker had the ability to trigger an OOM at a specific moment during JIT compilation. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131.	2024-10-01	8.8	High
CVE-2024-8885	sophos - Sophos Intercept X	A local privilege escalation vulnerability in Sophos Intercept X for Windows with Central Device Encryption 2024.2.0 and older allows writing of arbitrary files.	2024-10-02	8.8	High
CVE-2024-20393	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin.	2024-10-02	8.8	High
CVE-2024-20432	cisco - nexus_dashboard_fabric_controller	A vulnerability in the REST API and web UI of Cisco Nexus Dashboard Fabric Controller (NDFC) could allow an authenticated, low-privileged, remote attacker to perform a command injection attack against an affected device. This vulnerability is due to improper user authorization and insufficient validation of command arguments. An attacker could exploit this vulnerability by submitting crafted commands to an affected REST API endpoint or through the web UI. A successful exploit could allow the attacker to execute arbitrary commands on the CLI of a Cisco NDFC-managed device with network-admin privileges. Note: This vulnerability does not affect Cisco NDFC when it is configured for storage area network (SAN) controller deployment.	2024-10-02	8.8	High
CVE-2024-20449	cisco - nexus_dashboard_fabric_controller	A vulnerability in Cisco Nexus Dashboard Fabric Controller (NDFC) could allow an authenticated, remote attacker with low privileges to execute arbitrary code on an affected device. This vulnerability is due to improper path validation. An attacker could exploit this vulnerability by using the Secure Copy Protocol (SCP) to upload malicious code to an affected device using path traversal techniques. A successful exploit could allow the attacker to execute arbitrary code in a specific container with the privileges of root.	2024-10-02	8.8	High
CVE-2024-20448	cisco - nexus_dashboard_fabric_controller	A vulnerability in the Cisco Nexus Dashboard Fabric Controller (NDFC) software, formerly Cisco Data Center Network Manager (DCNM), could allow an attacker with access to a backup file to view sensitive information. This vulnerability is due to the improper storage of sensitive information within config only and full backup files. An attacker could exploit this vulnerability by parsing the contents of a backup file that is generated from an affected device. A successful exploit could allow the attacker to access sensitive information, including NDFC-connected device credentials, the NDFC site manager private key, and the scheduled backup file encryption key.	2024-10-02	8.6	High
CVE-2024-20490	cisco - multiple products	A vulnerability in a logging function of Cisco Nexus Dashboard Fabric Controller (NDFC) and Cisco Nexus Dashboard Orchestrator (NDO) could allow an attacker with access to a tech support file to view sensitive information. This vulnerability exists because HTTP proxy credentials could be recorded in an internal log that is stored in the tech support file. An attacker could exploit this vulnerability by accessing a tech support file that is generated from an affected system. A successful exploit could allow the attacker to view HTTP proxy server admin credentials in clear text that are configured on Nexus Dashboard	2024-10-02	8.6	High

		to reach an external network. Note: Best practice is to store debug logs and tech support files safely and to share them only with trusted parties because they may contain sensitive information.			
CVE-2024-20491	cisco - multiple products	A vulnerability in a logging function of Cisco Nexus Dashboard Insights could allow an attacker with access to a tech support file to view sensitive information. This vulnerability exists because remote controller credentials are recorded in an internal log that is stored in the tech support file. An attacker could exploit this vulnerability by accessing a tech support file that is generated from an affected system. A successful exploit could allow the attacker to view remote controller admin credentials in clear text. Note: Best practice is to store debug logs and tech support files safely and to share them only with trusted parties because they may contain sensitive information.	2024-10-02	8.6	High
CVE-2024-44193	apple - iTunes for Windows	A logic issue was addressed with improved restrictions. This issue is fixed in iTunes 12.13.3 for Windows. A local attacker may be able to elevate their privileges.	2024-10-02	8.4	High
CVE-2024-45772	apache - lucene	Deserialization of Untrusted Data vulnerability in Apache Lucene Replicator. This issue affects Apache Lucene's replicator module: from 4.4.0 before 9.12.0. The deprecated org.apache.lucene.replicator.http package is affected. The org.apache.lucene.replicator.nrt package is not affected. Users are recommended to upgrade to version 9.12.0, which fixes the issue. Java serialization filters (such as -Djdk.serialFilter='!*' on the commandline) can mitigate the issue on vulnerable versions without impacting functionality.	2024-09-30	8.0	High
CVE-2024-9393	mozilla - multiple products	An attacker could, via a specially crafted multipart response, execute arbitrary JavaScript under the `resource://pdf.js` origin. This could allow them to access cross-origin PDF content. This access is limited to "same site" documents by the Site Isolation feature on desktop clients, but full cross-origin access is possible on Android versions. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131.	2024-10-01	7.5	High
CVE-2024-9394	mozilla - multiple products	An attacker could, via a specially crafted multipart response, execute arbitrary JavaScript under the `resource://devtools` origin. This could allow them to access cross-origin JSON content. This access is limited to "same site" documents by the Site Isolation feature on desktop clients, but full cross-origin access is possible on Android versions. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131.	2024-10-01	7.5	High
CVE-2024-20498	cisco - meraki_mx65_firmware	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention.	2024-10-02	7.5	High
CVE-2024-20499	cisco - meraki_z4c_firmware	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention.	2024-10-02	7.5	High
CVE-2024-20500	cisco - meraki_z4c_firmware	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not	2024-10-02	7.5	High

		impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention.			
CVE-2024-20501	cisco - meraki_mx65_firmware	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention.	2024-10-02	7.5	High
CVE-2024-20502	cisco - meraki_mx65_firmware	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention.	2024-10-02	7.5	High
CVE-2024-41594	draytek - vigor2620_firmware	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL.	2024-10-03	7.5	High
CVE-2024-9403	mozilla - multiple products	Memory safety bugs present in Firefox 130. 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 < 131 and Thunderbird < 131.	2024-10-01	7.3	High
CVE-2024-47561	apache software foundation - Apache Avro Java SDK	Schema parsing in the Java SDK of Apache Avro 1.11.3 and previous versions allows bad actors to execute arbitrary code. Users are recommended to upgrade to version 1.11.4 or 1.12.0, which fix this issue.	2024-10-03	7.3	High
CVE-2024-20365	cisco - multiple products	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root.	2024-10-02	7.2	High
CVE-2024-20470	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system.	2024-10-02	7.2	High
CVE-2024-20516	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	2024-10-02	6.8	Medium
CVE-2024-20517	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by	2024-10-02	6.8	Medium

		sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.			
CVE-2024-20522	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	2024-10-02	6.8	Medium
CVE-2024-20523	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	2024-10-02	6.8	Medium
CVE-2024-20524	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	2024-10-02	6.8	Medium
CVE-2024-20492	cisco - multiple products	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices.	2024-10-02	6.7	Medium
CVE-2024-9355	red hat - multiple products	A vulnerability was found in Golang FIPS OpenSSL. This flaw allows a malicious user to randomly cause an uninitialized buffer length variable with a zeroed buffer to be returned in FIPS mode. It may also be possible to force a false positive match between non-equal hashes when comparing a trusted computed hmac sum to an untrusted input sum if an attacker can send a zeroed buffer in place of a pre-computed sum. It is also possible to force a derived key to be all zeros instead of an unpredictable value. This may have follow-on implications for the Go TLS stack.	2024-10-01	6.5	Medium
CVE-2024-20441	cisco - multiple products	A vulnerability in a specific REST API endpoint of Cisco NDFC could allow an authenticated, low-privileged, remote attacker to learn sensitive information on an affected device. This vulnerability is due to insufficient authorization controls on the affected REST API endpoint. An attacker could exploit this vulnerability by sending crafted API requests to the&nbsp;affected endpoint. A successful exploit could allow the attacker to download config only or full backup files and learn sensitive configuration information. This vulnerability only affects a specific REST API endpoint and does not affect the web-based management interface.	2024-10-02	6.5	Medium
CVE-2024-20515	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to obtain sensitive information from an affected device. This vulnerability is due to a lack of proper data protection mechanisms for certain configuration settings. An attacker with Read-Only Administrator privileges could exploit this vulnerability by browsing to a page that contains sensitive data. A successful exploit could allow the	2024-10-02	6.5	Medium

		attacker to view device credentials that are normally not visible to Read-Only Administrators.			
CVE-2024-9100	manageengine - Analytics Plus	Zohocorp ManageEngine Analytics Plus versions before 5410 and Zoho Analytics On-Premise versions before 5410 are vulnerable to Path traversal.	2024-10-03	6.5	Medium
CVE-2024-9397	mozilla - multiple products	A missing delay in directory upload UI could have made it possible for an attacker to trick a user into granting permission via clickjacking. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131.	2024-10-01	6.1	Medium
CVE-2024-41591	draytek - vigor2620_firmware	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS.	2024-10-03	6.1	Medium
CVE-2024-20385	cisco - multiple products	A vulnerability in the SSL/TLS implementation of Cisco Nexus Dashboard Orchestrator (NDO) could allow an unauthenticated, remote attacker to intercept sensitive information from an affected device. This vulnerability exists because the Cisco NDO Validate Peer Certificate site management feature validates the certificates for Cisco Application Policy Infrastructure Controller (APIC), Cisco Cloud Network Controller (CNC), and Cisco Nexus Dashboard only when a new site is added or an existing one is reregistered. An attacker could exploit this vulnerability by using machine-in-the-middle techniques to intercept the traffic between the affected device and Cisco NDO and then using a crafted certificate to impersonate the affected device. A successful exploit could allow the attacker to learn sensitive information during communications between these devices.	2024-10-02	5.9	Medium
CVE-2024-20509	cisco - meraki_mx65_firmware	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session with the affected device.	2024-10-02	5.9	Medium
CVE-2024-20444	cisco - nexus_dashboard_fabric_controller	A vulnerability in Cisco Nexus Dashboard Fabric Controller (NDFC), formerly Cisco Data Center Network Manager (DCNM), could allow an authenticated, remote attacker with network-admin privileges to perform a command injection attack against an affected device. This vulnerability is due to insufficient validation of command arguments. An attacker could exploit this vulnerability by submitting crafted command arguments to a specific REST API endpoint. A successful exploit could allow the attacker to overwrite sensitive files or crash a specific container, which would restart on its own, causing a low-impact denial of service (DoS) condition.	2024-10-02	5.5	Medium
CVE-2024-44204	apple - multiple products	A logic issue was addressed with improved validation. This issue is fixed in iOS 18.0.1 and iPadOS 18.0.1. A user's saved passwords may be read aloud by VoiceOver.	2024-10-04	5.5	Medium
CVE-2024-9341	red hat - multiple products	A flaw was found in Go. When FIPS mode is enabled on a system, container runtimes may incorrectly handle certain file paths due to improper validation in the containers/common Go library. This flaw allows an attacker to exploit symbolic links and trick the system into mounting sensitive host directories inside a container. This issue also allows attackers to access critical host files, bypassing the intended isolation between containers and the host system.	2024-10-01	5.4	Medium
CVE-2024-20438	cisco - multiple products	A vulnerability in the REST API endpoints of Cisco NDFC could allow an authenticated, low-privileged, remote attacker to read or write files on an affected device. This vulnerability exists because of missing authorization controls on some REST API endpoints. An attacker could exploit this vulnerability by sending crafted API requests to an affected endpoint. A successful exploit could allow the attacker to perform limited network-admin functions such as reading device configuration information, uploading files, and modifying uploaded files. Note: This vulnerability only affects a subset of REST API endpoints and does not affect the web-based management interface.	2024-10-02	5.4	Medium
CVE-2024-20442	cisco - multiple products	A vulnerability in the REST API endpoints of Cisco Nexus Dashboard could allow an authenticated, low-privileged, remote attacker to perform limited Administrator actions on an affected device. This vulnerability is due to insufficient authorization controls on some REST API endpoints. An attacker could exploit this vulnerability by sending crafted API requests to an affected endpoint. A successful exploit could allow the attacker to perform limited Administrator functions such as viewing portions of the web UI, generating config only or full backup files, and deleting tech support files. This vulnerability only affects a subset of REST API endpoints and does not affect the web-based management interface.	2024-10-02	5.4	Medium

CVE-2024-20477	cisco - multiple products	A vulnerability in a specific REST API endpoint of Cisco NDFC could allow an authenticated, low-privileged, remote attacker to upload or delete files on an affected device. This vulnerability exists because of missing authorization controls on the affected REST API endpoint. An attacker could exploit this vulnerability by sending crafted API requests to the affected endpoint. A successful exploit could allow the attacker to upload files into a specific container or delete files from a specific folder within that container. This vulnerability only affects a specific REST API endpoint and does not affect the web-based management interface.	2024-10-02	5.4	Medium
CVE-2024-41587	draytek - multiple products	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6.	2024-10-03	5.4	Medium
CVE-2024-9398	mozilla - multiple products	By checking the result of calls to \`window.open\` with specifically set protocol handlers, an attacker could determine if the application which implements that protocol handler is installed. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131.	2024-10-01	5.3	Medium
CVE-2024-20513	cisco - meraki_mx65_firmware	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate.	2024-10-02	5.3	Medium
CVE-2024-45073	ibm - WebSphere Application Server	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2024-09-30	4.8	Medium
CVE-2024-9407	red hat - multiple products	A vulnerability exists in the bind-propagation option of the Dockerfile RUN --mount instruction. The system does not properly validate the input passed to this option, allowing users to pass arbitrary parameters to the mount instruction. This issue can be exploited to mount sensitive directories from the host into a container during the build process and, in some cases, modify the contents of those mounted files. Even if SELinux is used, this vulnerability can bypass its protection by allowing the source directory to be relabeled to give the container access to host files.	2024-10-01	4.7	Medium
CVE-2024-44207	apple - multiple products	This issue was addressed with improved checks. This issue is fixed in iOS 18.0.1 and iPadOS 18.0.1. Audio messages in Messages may be able to capture a few seconds of audio before the microphone indicator is activated.	2024-10-04	4.3	Medium

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.