Advisory Alert

Alert Number: AAA20250206 **Date:** February 6, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
Dell	**High**	Linux Kernel Use-after-free Vulnerability
Juniper	**High**	Multiple Improper Handling of Exceptional Conditions
Cisco	**High**, Medium	Multiple Vulnerabilities
F5	**High**, Medium, Low	Multiple Vulnerabilities
Red Hat	Medium	Multiple Vulnerabilities
Synology	Medium	Security Update
Drupal	Medium	Cross Site Request Forgery Vulnerability
Nginx	Medium	SSL Session Reuse Vulnerability

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20124, CVE-2025-20125)
Description	Cisco has released security updates addressing multiple vulnerabilities in Cisco Identity Services Engine (ISE) that, if exploited, could allow an authenticated remote attacker to execute arbitrary commands and elevate privileges on an affected device. **CVE-2025-20124** - This vulnerability is due to insecure deserialization of user-supplied Java byte streams by the affected software. An attacker could exploit this vulnerability by sending a crafted serialized Java object to an affected API. A successful exploit could allow the attacker to execute arbitrary commands on the device and elevate privileges. **CVE-2025-20125** - This vulnerability is due to a lack of authorization in a specific API and improper validation of user-supplied data. An attacker could exploit this vulnerability by sending a crafted HTTP request to a specific API on the device. A successful exploit could allow the attacker to attacker to obtain information, modify system configuration, and reload the device. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco ISE Software Releases 3.0, 3.1, 3.2 and 3.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multivuls-FTW9AOXF

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Linux Kernel Use-after-free Vulnerability (CVE-2024-36971)
Description	Dell has released security updates addressing a Linux Kernel Use-after-free Vulnerability that exists in a third-party product affecting NetWorker vProxy. This vulnerability could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetWorker vProxy OVA versions 19.10 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000281334/dsa-2025-073-security-update-for-dell-networker-vproxy-linux-kernel-component-vulnerabilities

Affected Product	**Juniper**
Severity	**High**
Affected Vulnerability	Multiple Improper Handling of Exceptional Conditions (CVE-2024-39549, CVE-2024-39564)
Description	Juniper has released security updates addressing multiple Improper Handling of Exceptional Conditions that exist in the routing protocol daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved. These conditions allow a network based, attacker to cause the RPD process to crash leading to a Denial of Service (DoS). Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Junos OS: • All versions before 21.2R3-S8, • 21.4 before 21.4R3-S8, • 22.2 before 22.2R3-S5, • 22.3 before 22.3R3-S4, • 22.4 before 22.4R3-S4, • 23.2 before 23.2R2-S1, • 23.4 before 23.4R1-S2, 23.4R2. Junos OS Evolved: • All versions before 21.2R3-S8-EVO, • 21.4 before 21.4R3-S8-EVO, • 22.2 before 22.2R3-S5-EVO, • 22.3 before 22.3R3-S4-EVO, • 22.4 before 22.4R3-S4-EVO, • 23.2 before 23.2R2-S1-EVO, • 23.4 before 23.4R1-S2-EVO, 23.4R2-EVO.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-07-Security-Bulletin-Junos-OS-Receipt-of-malformed-BGP-path-attributes-leads-to-a-memory-leak-CVE-2024-39549?language=en_US

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20397, CVE-2025-20169, CVE-2025-20170, CVE-2025-20171, CVE-2025-20172, CVE-2025-20173, CVE-2025-20174, CVE-2025-20175, CVE-2025-20176, CVE-2025-20183, CVE-2025-20204, CVE-2025-20205, CVE-2025-20179, CVE-2025-20180, CVE-2025-20207, CVE-2025-20184, CVE-2025-20185)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of Service, Cross-Site Scripting, Security Restrictions Bypass, Information Disclosure and local or remote Arbitrary Command Execution. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• MDS 9000 Series Multilayer Switches (CSCwh76163) • Nexus 3000 Series Switches (CSCwm47438) • Nexus 7000 Series Switches (CSCwh76166) • Nexus 9000 Series Fabric Switches in ACI mode (CSCwn11901) • Nexus 9000 Series Switches in standalone NX-OS mode (CSCwm47438) • UCS 6400 Series Fabric Interconnects (CSCwj35846) • UCS 6500 Series Fabric Interconnects (CSCwj35846) • Cisco AsyncOS for Secure Web Appliance Software Releases 15.2, 15.1, 15.0, 14.5, 14.0 and earlier • Cisco ISE Software Release s 3.4, 3.3, 3.2, 3.1 and 3.0 • Cisco Expressway Series Releases 15, 14 and earlier • Cisco AsyncOS Software Release 16.0, 15.5, 15.0 and earlier • Cisco Secure Email and Web Manager Releases 16.0, 15.5 and earlier • Cisco Secure Email Gateway Releases 16.0, 15.5, 15.0 and earlier • Cisco Secure Web Appliance Releases 15.2, 15.1, 15.0 and earlier • Cisco devices if they are running a vulnerable release of Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software with the SNMP (versions 1, 2c, and 3) feature enabled. • (Use the Cisco IOS and IOS XE Software Checker to identify vulnerable versions)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-image-sig-bypas-pQDRQvjL • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-dos-sdxnSUcW • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-swa-range-bypass-2BsEHYSu • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-42tgsdMG • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-xss-uexUZrEW • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-xss-WCk2WcuG • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-wsa-snmp-inf-FqPvL8sX • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-wsa-multi-yKUJhS34

Affected Product	**F5**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-23413, CVE-2025-24319, CVE-2025-24312, CVE-2025-22846, CVE-2025-23239, CVE-2025-20029, CVE-2025-21087, CVE-2025-23415, 2025-20045, CVE-2025-21091, CVE-2025-23412, CVE-2025-24326, CVE-2025-20058, CVE-2025-24497, CVE-2025-22891, CVE-2025-24320)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of Service, Security Restrictions Bypass, Information Disclosure, Remote Command Injection. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next Central Manager versions 20.2.0 - 20.2.1 BIG-IP Next CNF versions 1.1.0 - 1.3.3 BIG-IP Next SPK versions 1.9.0, 1.8.0 - 1.8.2 and 1.7.0- 1.7.6 BIG-IP (AFM) versions 17.1.0 - 17.1.1, 16.1.4 - 16.1.5 and 15.1.0 - 15.1.10 BIG-IP (all modules) versions 17.1.0 - 17.1.2, 16.1.0 - 16.1.5 and 15.1.0 - 15.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000149185 • https://my.f5.com/manage/s/article/K000148412 • https://my.f5.com/manage/s/article/K000141380 • https://my.f5.com/manage/s/article/K000139780 • https://my.f5.com/manage/s/article/K000138757 • https://my.f5.com/manage/s/article/K000148587 • https://my.f5.com/manage/s/article/K000134888 • https://my.f5.com/manage/s/article/K000139656 • https://my.f5.com/manage/s/article/K000138932 • https://my.f5.com/manage/s/article/K000140933 • https://my.f5.com/manage/s/article/K000141003 • https://my.f5.com/manage/s/article/K000140950 • https://my.f5.com/manage/s/article/K000140947 • https://my.f5.com/manage/s/article/K000140920 • https://my.f5.com/manage/s/article/K000139778 • https://my.f5.com/manage/s/article/K000140578

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26935, CVE-2024-50275)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to directory regression and Linux kernel SVE stale CPU state. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Red Hat Enterprise Linux for x86_64 8 x86_64 • Red Hat Enterprise Linux for IBM z Systems 8 s390x • Red Hat Enterprise Linux for Power, little endian 8 ppc64le • Red Hat Enterprise Linux for ARM 64 8 aarch64 • Red Hat CodeReady Linux Builder for x86_64 8 x86_64 • Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le • Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 • Red Hat Enterprise Linux for Real Time 8 x86_64 • Red Hat Enterprise Linux for Real Time for NFV 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:1068 • https://access.redhat.com/errata/RHSA-2025:1067

Affected Product	**Synology**
Severity	**Medium**
Affected Vulnerability	Security Update
Description	Synology has released security updates addressing a vulnerability that exists in DiskStation Manager. This vulnerability allows man-in-the-middle attackers to hijack the authentication of administrators. Synology advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	DSM versions 7.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_25_01

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Cross Site Request Forgery Vulnerability
Description	Drupal has released security updates addressing a Cross Site Request Forgery vulnerability that exists in OAuth2 Client. This vulnerability could be exploited by malicious users to compromise the affected system. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Oauth2 Client module versions prior to 4.1.3 for Drupal 10 or 11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2025-013

Affected Product	**Nginx**
Severity	**Medium**
Affected Vulnerability	SSL Session Reuse Vulnerability (CVE-2025-23419)
Description	Nginx has released security updates addressing a SSL Session Reuse Vulnerability that exists in multiple Nginx versions. **CVE-2025-23419** - Insufficient check in virtual servers handling with TLSv1.3 SNI allowed to reuse SSL sessions in a different virtual server, to bypass client SSL certificates verification. Nginx advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Nginx versions 1.11.4 - 1.27.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nginx.org/en/CHANGES#:~:text=Changes%20with%20nginx%201.27.4,Bugfixes%20in%20HTTP/3

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.