Advisory Alert

Alert Number: AAA20250508 **Date:** May 8, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Arbitrary File Upload Vulnerability
Dell	**High**, **Medium**	Multiple Vulnerabilities
Drupal	**High**, **Medium**	Multiple Vulnerabilities
F5	**High**, **Medium**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**	Multiple Vulnerabilities
MariaDB	**Medium**	Multiple Vulnerabilities
FortiGuard	**Low**	Integer Overflow or Wraparound Vulnerability

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Arbitrary File Upload Vulnerability (CVE-2025-20188)
Description	Cisco has released security update addressing an Arbitrary File Upload Vulnerability that exists in Cisco IOS XE Wireless Controller Software. **CVE-2025-20188 -** This vulnerability is due to the presence of a hard-coded JSON Web Token (JWT) on an affected system. An attacker could exploit this vulnerability by sending crafted HTTPS requests to the AP image download interface. A successful exploit could allow the attacker to upload files, perform path traversal, and execute arbitrary commands with root privileges. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco products running vulnerable release of Cisco IOS XE Software • Catalyst 9800-CL Wireless Controllers for Cloud • Catalyst 9800 Embedded Wireless Controller for Catalyst 9300, 9400, and 9500 Series Switches • Catalyst 9800 Series Wireless Controllers • Embedded Wireless Controller on Catalyst APs
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-file-uplpd-rHZG9UfC

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-37343, CVE-2022-43505, CVE-2022-40982, CVE-2022-44611, CVE-2022-23908, CVE-2022-41804, CVE-2025-30101, CVE-2025-30102)
Description	Dell has released a security update addressing multiple vulnerabilities in their products. If exploited, These vulnerabilities could be exploited by malicious users to compromise affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerScale OneFS - Versions 9.4.0.0 through 9.10.1.0 PowerScale OneFS - Versions 9.8.0.0 through 9.10.1.0 Dell Edge Gateway 3200 Firmware - Versions prior to 2.00.10 Dell Networking VEP4600 – 4 Core Firmware - Versions prior to 4.3 Dell Networking VEP4600 – 8 Core Firmware - Versions prior to 4.3 Dell Networking VEP4600 – 16 Core Firmware - Versions prior to 4.3 Dell Edge Gateway 5200 Firmware - Versions prior to 2.00.10 PowerSwitch Z9664F-ON Firmware - Versions prior to 3.54.5.1-6 Dell EMC Networking VEP1425/VEP1445/VEP1485 Firmware - Versions prior to 2.6 Dell SD-WAN Edge 600 Firmware - Versions prior to 2.6 PowerSwitch Z9432F-ON Firmware - Versions prior to 3.51.5.1-18 PowerSwitch Z9264F-ON Firmware - Versions prior to 3.42.5.1-19 PowerSwitch S5448F-ON Firmware - Versions prior to 3.52.5.1-10 PowerSwitch E3200-ON Series Firmware - Versions prior to 3.57.5.1-4 PowerSwitch N2200-ON Series Firmware - Versions prior to 3.45.5.1-31 PowerSwitch N3200-ON Series Firmware - Versions prior to 3.45.0.9-10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000317419/dsa-2025-192-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000317839/dsa-2025-183-security-update-for-dell-networking-products-for-multiple-vulnerabilities

Affected Product	**Drupal**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-47710, CVE-2025-47709, CVE-2025-47708, CVE-2025-47707, CVE-2025-47706, CVE-2025-47705, CVE-2025-47704, CVE-2025-47703, CVE-2025-47702, CVE-2025-47701)
Description	Drupal has released security updates addressing Multiple Vulnerabilities that exist in their products. This vulnerability could be exploited by malicious users to Couse Cross Site Request Forgery (CSRF) attacks, Access Bypass, Cross Site Scripting. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/security

Affected Product	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-43878, CVE-2025-41399, CVE-2025-41414, CVE-2025-46265, CVE-2025-36557, CVE-2025-35995, CVE-2025-41433, CVE-2025-36546, CVE-2025-36525, CVE-2025-36504, CVE-2025-31644, CVE-2025-41431)
Description	F5 has released security updates addressing multiple vulnerabilities in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. F5 advises applying the security fixes as soon as possible to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000139502 • https://my.f5.com/manage/s/article/K000137709 • https://my.f5.com/manage/s/article/K000140968 • https://my.f5.com/manage/s/article/K000139503 • https://my.f5.com/manage/s/article/K000139571 • https://my.f5.com/manage/s/article/K000149952 • https://my.f5.com/manage/s/article/K000140937 • https://my.f5.com/manage/s/article/K000140574 • https://my.f5.com/manage/s/article/K000150598 • https://my.f5.com/manage/s/article/K000140919 • https://my.f5.com/manage/s/article/K000148591 • https://my.f5.com/manage/s/article/K000150668

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20140, CVE-2025-20186, CVE-2025-20154, CVE-2025-20191, CVE-2025-20122, CVE-2025-20182, CVE-2025-20197, CVE-2025-20198, CVE-2025-20192, CVE-2025-20162, CVE-2025-20164, CVE-2025-20202, CVE-2025-20210, CVE-2025-20181, CVE-2025-20189, CVE-2025-20193, CVE-2025-20194, CVE-2025-20147, CVE-2025-20216, CVE-2025-20151, CVE-2025-20221, CVE-2025-20187, CVE-2025-20213, CVE-2025-20214, CVE-2025-20137, CVE-2025-20196, CVE-2025-20190, CVE-2025-20223, CVE-2025-20157, CVE-2025-20155)
Description	Cisco has released security updates addressing multiple vulnerabilities in their products. If exploited, these vulnerabilities could lead to Remote Code Execution, Out-of-Band Access, Command Injection, Privilege Escalation. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/publicationListing.x?product=Cisco&sort=-day_sir&limit=50#~Vulnerabilities

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 18.04, Ubuntu 16.04, Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7496-1 • https://ubuntu.com/security/notices/USN-7498-1

Affected Product	**MariaDB**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-30722, CVE-2025-30693)
Description	MariaDB has released a security update addressing multiple vulnerabilities in their products. **CVE-2025-30722 -** Vulnerability in the MySQL Client product of Oracle MySQL (component: Client: mysqldump). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Client accessible data as well as unauthorized update, insert or delete access to some of MySQL Client accessible data. CVSS 3.1 Base Score 5.9 **CVE-2025-30693 -** Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 MariaDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	MariaDB 11.4.6, 10.6.22, 10.5.29, 10.11.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://mariadb.com/kb/en/mariadb-11-4-6-release-notes/ • https://mariadb.com/kb/en/mariadb-10-6-22-release-notes/ • https://mariadb.com/kb/en/mariadb-10-5-29-release-notes/ • https://mariadb.com/kb/en/mariadb-10-11-12-release-notes/

Affected Product	**FortiGuard**
Severity	**Low**
Affected Vulnerability	Integer Overflow or Wraparound Vulnerability (CVE-2024-46669)
Description	FortiGuard has released security updates addressing an Integer Overflow or Wraparound vulnerability that exist in their products. **CVE-2024-46669 -** An Integer Overflow or Wraparound vulnerability in FortiOS and FortiSASE FortiOS tenant IPsec IKEv1 service may allow an authenticated attacker to crash the IPsec tunnel via crafted requests, resulting in potential denial of service. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiOS 7.4 - 7.4.0 through 7.4.4 FortiOS 7.2 - 7.2.0 through 7.2.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-24-267

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.