Advisory Alert

Alert Number: **AAA20250306** **Date:** **March 6, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	DLL Hijacking Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Juniper	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Dell	**Medium**	Signature Verification Vulnerability
cPanel	**Medium**	Security Update
Drupal	**Medium**	Access Bypass Vulnerability

Description

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	DLL Hijacking Vulnerability (CVE-2025-20206)
Description	Cisco has released security updates addressing a DLL Hijacking Vulnerability that exists in their Cisco Secure Client for Windows. **CVE-2025-20206**- A vulnerability in the interprocess communication (IPC) channel of Cisco Secure Client for Windows exists due to insufficient validation of resources loaded by the application at runtime. This vulnerability could allow an authenticated local attacker to perform a DLL hijacking attack on an affected device if the Secure Firewall Posture Engine, formerly HostScan, is installed on Cisco Secure Client. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Secure Client Release Earlier than 5.1.8.105 for Windows when it has the Secure Firewall Posture Engine installed.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-dll-injection-AOyzEqSg

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52924, CVE-2023-52925, CVE-2024-26708, CVE-2024-26810, CVE-2024-41055, CVE-2024-44974, CVE-2024-45009, CVE-2024-45010, CVE-2024-47701, CVE-2024-49884, CVE-2024-49950, CVE-2024-50073, CVE-2024-50085, CVE-2024-50115, CVE-2024-50185, CVE-2024-53147, CVE-2024-53173, CVE-2024-53226, CVE-2024-53239, CVE-2024-56539, CVE-2024-56548, CVE-2024-56568, CVE-2024-56579, CVE-2024-56605, CVE-2024-56647, CVE-2024-56720, CVE-2024-57889, CVE-2024-57948, CVE-2025-21636, CVE-2025-21637, CVE-2025-21638, CVE-2025-21639, CVE-2025-21640, CVE-2025-21647, CVE-2025-21680, CVE-2025-21684, CVE-2025-21687, CVE-2025-21688, CVE-2025-21689, CVE-2025-21690, CVE-2025-21692, CVE-2025-21697, CVE-2025-21699, CVE-2025-21700)
Description	SUSE 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. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Confidential Computing Module 15-SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2025/suse-su-20250784-1/

Affected Product	**Juniper**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-25745, CVE-2021-25746, CVE-2021-25748, CVE-2021-44225, CVE-2022-23471, CVE-2022-23524, CVE-2022-23525, CVE-2022-23526, CVE-2022-4886, CVE-2023-25153, CVE-2023-25173, CVE-2023-28840, CVE-2023-28841, CVE-2023-28842, CVE-2023-32732, CVE-2023-33953, CVE-2023-4785, CVE-2023-5043, CVE-2024-24557)
Description	Juniper 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. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Juniper Networks BBE Cloudsetup
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-07-Security-Bulletin-BBE-Cloudsetup-Multiple-vulnerabilities-resolved-in-2-1-0-release?language=en_US

Affected Product	**Ubuntu**
Severity	**High** , **Medium**, **Low**
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 24.10 Ubuntu 24.04 LTS Ubuntu 22.04 LTS Ubuntu 20.04 LTS Ubuntu 16.04 ESM Ubuntu 14.04 ESM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7333-1 • https://ubuntu.com/security/notices/USN-7332-1 • https://ubuntu.com/security/notices/USN-7331-1 • https://ubuntu.com/security/notices/USN-7327-1 • https://ubuntu.com/security/notices/USN-7324-1 • https://ubuntu.com/security/notices/USN-7323-1 • https://ubuntu.com/security/notices/USN-7322-1

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Signature Verification Vulnerability (CVE-2024-36347)
Description	Dell has released security updates addressing a Signature Verification Vulnerability that exists in Dell AMD-based PowerEdge Server. Which could be exploited by malicious users to compromise the affected system. **CVE-2024-36347**- Improper signature verification in AMD CPU ROM microcode patch loader may allow an attacker with local administrator privilege to load malicious microcode, potentially resulting in loss of integrity of x86 instruction execution, loss of confidentiality and integrity of data in x86 CPU privileged context and compromise of SMM execution environment. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• PowerEdge R6615, R7615, R6625, R7625, XC Core XC7625: BIOS versions prior to 1.11.2. • PowerEdge C6615: BIOS versions prior to 1.6.2. • PowerEdge R6515, R6525, R7515, R7525, C6525, Dell EMC XC Core XC7525: BIOS versions prior to 2.18.1. • PowerEdge XE8545: BIOS versions prior to 2.17.1. • PowerEdge R6415, R7415, R7425: BIOS versions prior to 1.24.0.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000291174/dsa-2025-112-security-update-for-dell-amd-based-poweredge-server-vulnerability

Affected Product	**cPanel**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2025-27111)
Description	cPanel has released a security update, including an Escape Sequence Injection vulnerability in all versions of Ruby Rack up to 2.2.11 for EasyApache 4. These vulnerabilities could be exploited by malicious users to compromise the affected system. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	EasyApache 4 All versions of Ruby Rack through 2.2.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-v25-8-maintenance-and-security-release/

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Access Bypass Vulnerability
Description	Drupal has released security updates addressing an Access Bypass Vulnerability in the Two-factor Authentication (TFA) module for Drupal 8.x. The vulnerability exists due to a flaw in the module, which does not sufficiently ensure that known login routes are not overridden by third-party modules, allowing an attacker to bypass authentication. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Two-factor Authentication (TFA) module version prior to 1.10.0 for Drupal 8.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2025-023

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.