Advisory Alert

Alert Number: AAA20250408 **Date:** April 8, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Cisco	**High**	Image Verification Bypass Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-29499, CVE-2024-6387, CVE-2024-38433, CVE-2023-22351, CVE-2024-21871, CVE-2023-25546, CVE-2023-42772, CVE-2024-21829, CVE-2024-21781, CVE-2023-41833, CVE-2023-43753, CVE-2024-23984, CVE-2024-24968, CVE-2024-38303, CVE-2024-38304, CVE-2024-24853)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third-party products, which in turn affect Dell products. These vulnerabilities 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	Dell Avamar Data Store Gen5A Operating System Version - ADS Gen5A
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000304933/dsa-2025-167-security-update-for-dell-avamar-data-store-gen5a-multiple-third-party-component-vulnerabilities

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Image Verification Bypass Vulnerability (CVE-2024-20397)
Description	Cisco has released security updates addressing an image verification bypass vulnerability that exists in their products. **CVE-2024-20397 -** A vulnerability in the bootloader of Cisco NX-OS Software could allow an unauthenticated attacker with physical access to an affected device, or an authenticated, local attacker with administrative credentials, to bypass NX-OS image signature verification. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	This vulnerability affects the following Cisco products if they are running a release of Cisco NX-OS Software that includes a vulnerable BIOS version, • MDS 9000 Series Multilayer Switches • Nexus 3000 Series Switches • Nexus 7000 Series Switches • Nexus 9000 Series Fabric Switches in ACI mode • Nexus 9000 Series Switches in standalone NX-OS mode • UCS 6400 Series Fabric Interconnects • UCS 6500 Series Fabric Interconnects
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

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.