Advisory Alert

Alert Number: **AAA20250310** **Date:** **March 10, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Multiple Vulnerabilities
Commvault	**High**	Security Update
QNAP	**Medium, Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-39279, CVE-2024-28047, CVE-2024-36293)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products, which affects Dell PowerEdge Server and EMC. **CVE-2024-39279** - Insufficient granularity of access control in UEFI firmware in some Intel processors may allow an authenticated user to potentially enable denial of service via local access. **CVE-2024-28047** - Improper input validation in UEFI firmware for some Intel Processors may allow a privileged user to potentially enable information disclosure via local access. **CVE-2024-36293** - Improper access control in the EDECCSSA user leaf function for some Intel® Processors with Intel SGX may allow an authenticated user to potentially enable denial of service via local access. Dell 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.dell.com/support/kbdoc/en-us/000283897/dsa-2025-041-security-update-for-dell-poweredge-server-for-intel-2025-security-advisories-2025-1-ipu

Affected Product	**Commvault**
Severity	**High**
Affected Vulnerability	Security Update
Description	Commvault has released security updates addressing a vulnerability that exists in all supported versions of the Commvault software. Webservers can be compromised through bad actors creating and executing webshells. Commvault advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Below Commvault versions on Linux and Windows 11.36.0 - 11.36.45 11.32.0 - 11.32.87 11.28.0 - 11.28.140 11.20.0 - 11.20.216
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://documentation.commvault.com/securityadvisories/CV_2025_03_1.html

Affected Product	**QNAP**
Severity	**Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53694, CVE-2024-53696, CVE-2024-38638, CVE-2024-50405, CVE-2024-53692, CVE-2024-53693, CVE-2024-53697, CVE-2024-53698, CVE-2024-53699, CVE-2024-48864, CVE-2024-50390, CVE-2024-13086, CVE-2024-53695, CVE-2024-53700)
Description	QNAP has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Information Disclosure, memory corruption, access bypass, data modification, arbitrary command execution. QNAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QVPN Device Client for Mac 2.2.x Qsync Client for Mac 5.1.x Qfinder Pro for Mac 7.11.x QuLog Center 1.7.x QuLog Center 1.8.x QTS 5.x QuTS hero h4.5.x QuTS hero h5.1.x QuTS hero h5.2.x File Station 5 version 5.x QuRouter 2.4.x HBS 3 Hybrid Backup Sync 25.1.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.qnap.com/en/security-advisory/qsa-24-51 • https://www.qnap.com/en/security-advisory/qsa-24-53 • https://www.qnap.com/en/security-advisory/qsa-24-52 • https://www.qnap.com/en/security-advisory/qsa-24-54 • https://www.qnap.com/en/security-advisory/qsa-24-55 • https://www.qnap.com/en/security-advisory/qsa-25-01 • https://www.qnap.com/en/security-advisory/qsa-25-03 • https://www.qnap.com/en/security-advisory/qsa-25-06 • https://www.qnap.com/en/security-advisory/qsa-25-07

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.