Advisory Alert

Alert Number: AAA20260212 **Date:** February 12, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
QNAP	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Dell	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
Palo Alto	**Medium**, **Low**	Multiple Vulnerabilities
Commvault	**Low**	Memory Disclosure Vulnerability

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released a security update 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 these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Basesystem Module 15-SP7 Development Tools Module 15-SP7 Legacy Module 15-SP7 SUSE Linux Enterprise Desktop 15 SP7 SUSE Linux Enterprise High Availability Extension 15 SP7 SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP7 SUSE Linux Enterprise Workstation Extension 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20260447-1/

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45801, CVE-2025-36379, CVE-2025-36377, CVE-2025-36376, CVE-2026-21441, CVE-2025-65945, CVE-2025-15284, CVE-2025-66418, CVE-2025-66471, CVE-2025-67735)
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Security QRadar EDR versions 3.12 to 3.12.23
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7260390 https://www.ibm.com/support/pages/node/7260392

Affected Product	**QNAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-54155, CVE-2025-54161, CVE-2025-54162, CVE-2025-62853, CVE-2025-66278, CVE-2026-22894, CVE-2025-62855, CVE-2025-62856, CVE-2025-54163, CVE-2025-54169, CVE-2025-57707, CVE-2025-57713, CVE-2025-62854, CVE-2025-30269, CVE-2025-54170, CVE-2025-30276, CVE-2025-47209, CVE-2025-48722, CVE-2025-53598, CVE-2025-54146, CVE-2025-54147, CVE-2025-54148, CVE-2025-58472, CVE-2025-30266, CVE-2025-48723, CVE-2025-48724, CVE-2025-52868, CVE-2025-52869, CVE-2025-52870, CVE-2025-57709, CVE-2025-54149, CVE-2025-54150, CVE-2025-54151, CVE-2025-54152, CVE-2025-57708, CVE-2025-57710, CVE-2025-57711, CVE-2025-58471, CVE-2024-42516, CVE-2024-43204, CVE-2024-43394, CVE-2024-47252, CVE-2025-23048, CVE-2025-49630, CVE-2025-49812, CVE-2025-53020, CVE-2025-54090, CVE-2025-47205, CVE-2025-58466, CVE-2025-66277, CVE-2025-48725, CVE-2025-59386, CVE-2025-66274, CVE-2025-10230, CVE-2025-9640, CVE-2025-58467, CVE-2025-58470, CVE-2025-68406)
Description	QNAP has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to conduct Path traversal, Denial of Service (DoS), Static Code Injection, Out-of-bounds read and Buffer overflow attacks. QNAP advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	File Station 5 version 5.5.x Qsync Central 5.0.x QTS 5.2.x QuTS hero h5.2.x and h5.3.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-26-03 https://www.qnap.com/en/security-advisory/qsa-26-02 https://www.qnap.com/en/security-advisory/qsa-26-04 https://www.qnap.com/en/security-advisory/qsa-26-05 https://www.qnap.com/en/security-advisory/qsa-26-08 https://www.qnap.com/en/security-advisory/qsa-26-06

Affected Product	**Dell**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23857, CVE-2025-27560, CVE-2025-30513, CVE-2025-32007, CVE-2025-32467, CVE-2025-27572, CVE-2025-27940, CVE-2025-31944, CVE-2025-31648, CVE-2025-22885, CVE-2025-29950, CVE-2025-52533, CVE-2024-21961, CVE-2025-48514, CVE-2025-29939, CVE-2025-48509, CVE-2025-0031, CVE-2025-52536, CVE-2024-21953, CVE-2024-36310, CVE-2024-36355, CVE-2025-54514, CVE-2025-29946, CVE-2025-29948, CVE-2025-29952, CVE-2025-48517, CVE-2025-0029, CVE-2025-0012, CVE-2025-52534, CVE-2025-32008, CVE-2025-20080, CVE-2025-27708)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party components utilized by their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply these security fixes at your earliest to protect your 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/000426781/dsa-2026-081-security-update-for-dell-update-package-dup-framework-vulnerability • https://www.dell.com/support/kbdoc/en-us/000426775/dsa-2026-014-security-update-for-dell-poweredge-server-for-intel-server-firmware-vulnerability • https://www.dell.com/support/kbdoc/en-us/000426748/dsa-2026-027-security-update-for-dell-poweredge-server-for-intel-2026-security-advisories-2026-1-ipu • https://www.dell.com/support/kbdoc/en-us/000426743/dsa-2026-012-security-update-for-dell-poweredge-server-for-intel-2026-security-advisories-2026-1-ipu • https://www.dell.com/support/kbdoc/en-us/000426734/dsa-2026-011-security-update-for-dell-poweredge-server-for-intel-2025-security-advisories-2025-4-ipu • https://www.dell.com/support/kbdoc/en-us/000426703/dsa-2026-026-security-update-for-dell-amd-based-poweredge-server-vulnerability • https://www.dell.com/support/kbdoc/en-us/000390619/dsa-2026-010

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38022, CVE-2025-38568, CVE-2025-40294, CVE-2025-40322, CVE-2022-49503, CVE-2023-53192, CVE-2023-53673, CVE-2025-40251, CVE-2023-53751, CVE-2025-40304, CVE-2022-50673, CVE-2023-53833, CVE-2025-68301, CVE-2022-50865, CVE-2025-38051, CVE-2025-40096, CVE-2025-40258, CVE-2025-68285, CVE-2025-40154, CVE-2025-40240)
Description	Red Hat 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. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:2594 • https://access.redhat.com/errata/RHSA-2026:2573 • https://access.redhat.com/errata/RHSA-2026:2560 • https://access.redhat.com/errata/RHSA-2026:2558 • https://access.redhat.com/errata/RHSA-2026:2557 • https://access.redhat.com/errata/RHSA-2026:2535

Affected Product	**Palo Alto**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-0229, CVE-2026-0228)
Description	Palo Alto has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-0229**: A denial-of-service (DoS) vulnerability in the Advanced DNS Security (ADNS) feature of Palo Alto Networks PAN-OS® software enables an unauthenticated attacker to initiate system reboots using a maliciously crafted packet. Repeated attempts to initiate a reboot causes the firewall to enter maintenance mode. **CVE-2026-0228:** An improper certificate validation vulnerability in PAN-OS allows users to connect Terminal Server Agents on Windows to PAN-OS using expired certificates even if the PAN-OS configuration would not normally permit them to do so. Palo Alto advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PAN-OS 12.1 versions prior to 12.1.4 PAN-OS 11.2 versions prior to 11.2.10 PAN-OS 11.1 versions prior to 11.1.11 PAN-OS 10.2 versions prior to 10.2.17
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2026-0229 https://security.paloaltonetworks.com/CVE-2026-0228

Affected Product	**Commvault**
Severity	**Low**
Affected Vulnerability	Memory Disclosure Vulnerability (CVE-2025-14847)
Description	Commvault has released a security update addressing a memory disclosure vulnerability that exist in their products. CVE-2025-14847: This vulnerability affects MongoDB's handling of zlib compression, which under certain conditions may allow memory disclosure. Commvault advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Commvault versions: • 11.32.0 to 11.32.128 • 11.36.0 to 11.36.89 • 11.40.0 to 11.40.36
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://documentation.commvault.com/securityadvisories/CV_2026_02_1.html

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.