TLP: WHITE

Advisory Alert

Alert Number: AAA20251110 **Date:** November 10, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
QNAP	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Linux Kernel Vulnerabilities
QNAP	**High**, **Medium**	Multiple Vulnerabilities
IBM	**Medium**	Information Exposure Vulnerability
Red Hat	**Medium**	Multiple Vulnerabilities
NetApp	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**QNAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-59389, CVE-2025-62840, CVE-2025-62842, CVE-2025-62847, CVE-2025-62848, CVE-2025-62849, CVE-2025-11837)
Description	QNAP has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected products. QNAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QNAP Malware Remover 6.6.x QNAP Hyper Data Protector 2.2.x QNAP HBS 3 Hybrid Backup Sync prior to 26.1.x QNAP QTS 5.2.x, QuTS hero h5.2.x, QuTS hero h5.3.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.qnap.com/en/security-advisory/qsa-25-48 • https://www.qnap.com/en/security-advisory/qsa-25-46 • https://www.qnap.com/en/security-advisory/qsa-25-45 • https://www.qnap.com/en/security-advisory/qsa-25-47

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Linux Kernel Vulnerabilities (CVE-2025-38618, CVE-2025-38664, CVE-2025-38453, CVE-2025-38511, CVE-2025-38617, CVE-2024-53164)
Description	SUSE has released security updates addressing multiple linux kernel vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected products. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.6 SUSE Linux Enterprise Server 15 SP6, 15 SP7 SUSE Linux Enterprise Real Time 15 SP6, 15 SP7 SUSE Linux Enterprise Live Patching 15-SP6, 15-SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP6, 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20253987-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20253995-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20253998-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254000-1/

Affected Product	**QNAP**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-57712, CVE-2025-58463, CVE-2025-58465, CVE-2025-54168, CVE-2025-58469, CVE-2025-54167, CVE-2025-47207, CVE-2025-53408, CVE-2025-53409, CVE-2025-53410, CVE-2025-53411, CVE-2025-53412, CVE-2025-53413, CVE-2025-52865, CVE-2025-57706)
Description	QNAP has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected products. QNAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QuLog Center 1.8.x Qsync Central 5.0.x File Station 5 version 5.5.x Download Station 5.10.x (for QTS 5.2.1), (for QuTS hero h5.2.1) Notification Center 2.1.x (for QuTS hero h5.3.x) Notification Center 3.0.x (for QuTS hero h5.6.x, h6.0.x) Notification Center 1.9.x (for QTS 5.2.x, QuTS hero h5.2.x)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.qnap.com/en/security-advisory/qsa-25-41 • https://www.qnap.com/en/security-advisory/qsa-25-37 • https://www.qnap.com/en/security-advisory/qsa-25-42 • https://www.qnap.com/en/security-advisory/qsa-25-40 • https://www.qnap.com/en/security-advisory/qsa-25-38

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Information Exposure Vulnerability (CVE-2025-36131)
Description	IBM has released a security update addressing an information exposure vulnerability that exists in their products. **CVE-2025-36131 -** IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) clpplus command exposes user credentials to the terminal which could be obtained by a third party with physical access to the system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Versions 11.1.0 - 11.1.4.7, 11.5.0 - 11.5.9, 12.1.0 - 12.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7250484

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-36350, CVE-2024-36357, CVE-2025-40300, CVE-2024-28956, CVE-2025-39864)
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 products. Red Hat 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://access.redhat.com/errata/RHSA-2025:19930 • https://access.redhat.com/errata/RHSA-2025:19962

Affected Product	**NetApp**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-4207, CVE-2024-10977)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-4207 -** Multiple NetApp products incorporate PostgreSQL. PostgreSQL versions prior to 17.5, prior to 16.9, prior to 15.13, prior to 14.18, and prior to 13.21 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS). **CVE-2024-10977 -** Multiple NetApp products incorporate PostgreSQL. Certain versions of PostgreSQL are susceptible to a vulnerability which when successfully exploited could lead to addition or modification of data. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Brocade SAN Navigator (SANnav) - Versions SANnav 2.4.0a. Brocade SAN Navigator (SANnav) - Versions prior to SANnav 2.4.0b and SANnav 3.0.0.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20251107-0003 • https://security.netapp.com/advisory/ntap-20251107-0002

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.