Advisory Alert

Alert Number: AAA20260323 **Date:** March 23, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
QNAP	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Ubuntu	**High, Medium**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
NetApp	**Medium**	Denial of Service Vulnerability
QNAP	**Medium**	Cross Site Scripting Vulnerability

Description

Affected Product	**QNAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-62843, CVE-2025-62844, CVE-2025-62845, and CVE-2025-62846, CVE-2026-22897, CVE-2026-22900, CVE-2026-22901, CVE-2026-22902)
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 systems. QNAP advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	QuNetSwitch 2.0.x – Versions prior to 2.0.4.0415 QuNetSwitch 2.0.x – Versions prior to 2.0.5.0906 QuRouter 2.6.x – Versions prior to 2.6.3.009
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.qnap.com/en/security-advisory/qsa-26-12 • https://www.qnap.com/en/security-advisory/qsa-26-11

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-71085, CVE-2025-68813, CVE-2025-68285, CVE-2025-68284, CVE-2025-40297, CVE-2025-40284, CVE-2025-40258, CVE-2025-38488, CVE-2025-38159)
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 systems. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2026/suse-su-20260945-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260944-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260943-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260941-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260940-1/

Affected Product	**Ubuntu**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerability (CVE-2025-40215, CVE-2025-21704, CVE-2024-56593, CVE-2024-56581, CVE-2024-56548, CVE-2024-49927, CVE-2024-47659, CVE-2022-49267, CVE-2022-48875, CVE-2021-47599)
Description	Ubuntu 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 systems. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu – Versions 18.04 and 16.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8112-1

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Muliple Vulnerabilities (CVE-2025-38248, CVE-2026-23001)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in the kernel of their products. **CVE-2025-38248:** A local user could trigger a use-after-free vulnerability, a type of memory corruption, by improperly configuring network bridge router ports. This issue arises because the system fails to correctly remove ports from its internal router port lists, leading to references to freed memory. Exploiting this flaw could result in system instability, denial of service, or potentially allow for privilege escalation. **CVE-2026-23001:** A use-after-free can occur in macvlan source-mode forwarding when a source hash entry is deleted while the transmit/forwarding path still dereferences entry.vlan without proper RCU protection. A local attacker who can configure macvlan networking can race deletion with packet processing to crash the kernel and potentially achieve memory corruption. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:5197

Affected Product	**NetApp**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2025-9714)
Description	NetApp has released a security update addressing a vulnerability that exists in their product. **CVE-2025-9714**: Uncontrolled recursion in XPath evaluation in libxml2, allows a local attacker to cause a stack overflow via crafted expressions. XPath processing functions `xmlXPathRunEval`, `xmlXPathCtxtCompile`, and `xmlXPathEvalExpr` were resetting recursion depth to zero before making potentially recursive calls. When such functions were called recursively this could allow for uncontrolled recursion and lead to a stack overflow. NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	ONTAP 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20260320-0006

Affected Product	**QNAP**
Severity	**Medium**
Affected Vulnerability	Cross Site Scripting Vulnerability (CVE-2026-22895)
Description	QNAP has released a security update addressing a vulnerability that exists in their Product. **CVE-2026-22895:** If a remote attacker gains an administrator account, they can then exploit the vulnerability to bypass security mechanisms or read application data. QNAP advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	QuFTP Service 1.4.x – Versions prior to 1.4.3 QuFTP Service 1.5.x – Versions prior to 1.5.2 QuFTP Service 1.6.x – Versions prior to 1.6.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-26-15

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.