Advisory Alert

Alert Number: AAA202604022 **Date:** April 22, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Oracle	**Critical**	Multiple Vulnerabilities
QNAP	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
Oracle	**High**, **Medium**, **Low**	Multiple Vulnerabilities
QNAP	**Medium**	Cross-Site Scripting Vulnerability
IBM	**Medium**	Unrestricted Executable File Upload Vulnerability

Description

Affected Product	**Oracle**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-6965, CVE-2025-68615, CVE-2026-25968, CVE-2025-48913, CVE-2025-12543, CVE-2024-5535, CVE-2025-55130, CVE-2025-58050, CVE-2025-56005, CVE-2026-2760)
Description	Oracle has released security updates addressing multiple vulnerabilities that exist in the third-party components of their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Oracle advises to apply security fixes at your earliest to protect systems from potential threats.

Affected Products	Oracle Communications:
	• Cloud Native Core
	  ○ Network Exposure Function
	  ○ Unified Data Repository
	  ○ Network Slice Selection Function
	  ○ Policy
	• EAGLE
	• EAGLE Application Processor
	• EAGLE LNP Application Processor
	• LSMS
	• Messaging Server
	• Operations Monitor
	• Policy Management
	• Unified Assurance
	Oracle Solaris

Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.oracle.com/security-alerts/cpuapr2026.html • https://www.oracle.com/security-alerts/bulletinapr2026.html

Affected Product	**QNAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-22898, CVE-2026-22897, CVE-2026-22900, CVE-2026-22901, CVE-2026-22902, CVE-2025-62843, CVE-2025-62844, CVE-2025-62846, CVE-2025-62845)
Description	QNAP has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. QNAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QuRouter 2.6.x prior to 2.6.3.009 QuNetSwitch 2.0.x prior to 2.0.4.0415 QuNetSwitch 2.0.x prior to 2.0.5.0906 QVR Pro 2.7.x prior to 2.7.4.1485
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.qnap.com/en/security-advisory/qsa-26-07 • https://www.qnap.com/en/security-advisory/qsa-26-11 • https://www.qnap.com/en/security-advisory/qsa-26-12

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40309, CVE-2026-23268, CVE-2026-23191)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in the kernel component of their products. **CVE-2025-40309** – This vulnerability occurs due to a use-after-free error within the Bluetooth subsystem. It occurs when the system attempts to access or modify a connection object that has already been deleted from memory. If exploited, this flaw can lead to a system crash (denial of service) or potentially allow an attacker to execute malicious code with high-level system privileges. **CVE-2026-23268** – This vulnerability allows an unprivileged user to gain full control over system security policies by tricking a high-privilege program into performing actions on its behalf. By passing a specific file handle to a privileged process, the attacker can bypass standard security restrictions. **CVE-2026-23191** – This vulnerability involves a race condition in the Linux audio driver where simultaneous actions can overlap. This allows the system to access memory that has already been cleared. If triggered, this flaw can lead to a system crash or allow an attacker to destabilize the kernel to gain unauthorized control. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.6 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP6, 15-SP7 SUSE Linux Enterprise Real Time 15 SP6, 15 SP7 SUSE Linux Enterprise Server 12 SP5, 15 SP6, 15 SP7 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP6, 15 SP7 SUSE Linux Enterprise High Performance Computing 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20261505-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20261513-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20261527-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20261531-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20261532-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20261535-1/

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40064, CVE-2025-40168, CVE-2026-23204, CVE-2026-23231, CVE-2025-39766, CVE-2025-68741)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the kernel component of their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 10 x86_64 Red Hat Enterprise Linux for IBM z Systems 10 s390x Red Hat Enterprise Linux for Power, little endian 10 ppc64le Red Hat Enterprise Linux for ARM 64 10 aarch64 Red Hat CodeReady Linux Builder for x86_64 10 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le Red Hat CodeReady Linux Builder for ARM 64 10 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6, 8.8 x86_64 Red Hat Enterprise Linux Server - AUS 8.2, 8.6 x86_64 Red Hat Enterprise Linux Server - TUS 8.6, 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6, 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6, 8.8 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:9513 https://access.redhat.com/errata/RHSA-2026:9514 https://access.redhat.com/errata/RHSA-2026:9515 https://access.redhat.com/errata/RHSA-2026:9264

Affected Product	**Oracle**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle has released security updates addressing multiple vulnerabilities that exist in the third-party components of their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Oracle 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.oracle.com/security-alerts/cpuapr2026.html • https://www.oracle.com/security-alerts/bulletinapr2026.html

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 products. **CVE-2026-22895** - A cross-site scripting (XSS) vulnerability has been reported to affect QuFTP Service. 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 security fixes at your earliest to protect systems from potential threats.
Affected Products	QuFTP Service versions prior to 1.4.3, 1.5.2 and 1.6.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-26-15

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Unrestricted Executable File Upload Vulnerability (CVE-2025-36074)
Description	IBM has released a security update addressing a vulnerability that exists in their Security Verify products. **CVE-2025-36074** - IBM Security Verify Directory could be vulnerable to malicious file upload by not validating file type. A privileged user could upload malicious files into the system that can be sent to victims for performing further attacks against the system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security Verify Governance Identity Manager Adapters versions 10.0.1-10.0.18
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7270066

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.