TLP: WHITE

Advisory Alert

Alert Number: AAA20260512 **Date:** May 12, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Ubuntu	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
QNAP	Medium	Privilege Escalation Vulnerability

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-28780, CVE-2025-62718, CVE-2025-68121, CVE-2025-69264, CVE-2026-1525, CVE-2026-2332, CVE-2026-25547, CVE-2026-29045, CVE-2026-29145, CVE-2026-32635, CVE-2026-33210, CVE-2026-33228, CVE-2026-33701, CVE-2026-33896, CVE-2026-33937, CVE-2026-34520, CVE-2026-39324, CVE-2026-40477, CVE-2026-40478, CVE-2026-41242, CVE-2026-4800)
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 systems. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM HTTP Server version 8.5 and 9.0 API Connect V12 OnPrem version 12.1.0.0 to 12.1.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7272621 • https://www.ibm.com/support/pages/node/7272626

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-31431, CVE-2026-43284)
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 systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 • Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x • Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le • Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 • Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 • Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.4 aarch64 • Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 • Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x • Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.4 s390x • Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x • Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10, 9.4 and 9.6 ppc64le • Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 and 9.6 ppc64le • Red Hat Enterprise Linux for Power, little endian 8 and 9 ppc64le • Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.4 and 9.6 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 and 9.6 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6 and 8.8 x86_64 • Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6, 8.8, 9.4 and 9.6 x86_64 • Red Hat Enterprise Linux for x86_64 8 and 9 x86_64 • Red Hat Enterprise Linux Server - AUS 9.4 and 9.6 x86_64 • Red Hat Enterprise Linux Server - TUS 8.8 x86_64 • Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6, 8.8, 9.4 and 9.6 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:16111 • https://access.redhat.com/errata/RHSA-2026:16100 • https://access.redhat.com/errata/RHSA-2026:16063 • https://access.redhat.com/errata/RHSA-2026:16061 • https://access.redhat.com/errata/RHSA-2026:16018 • https://access.redhat.com/errata/RHSA-2026:15978 • https://access.redhat.com/errata/RHSA-2026:15976

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-11187, CVE-2025-15467, CVE-2025-15468, CVE-2025-15469, CVE-2025-66199, CVE-2025-68160, CVE-2025-69418, CVE-2025-69419, CVE-2025-69420, CVE-2025-69421, CVE-2026-22795, CVE-2026-22796, CVE-2026-3909, CVE-2026-3910, CVE-2026-5281, CVE-2025-31648, CVE-2025-30513, CVE-2025-31944, CVE-2025-32007, CVE-2025-32467, CVE-2025-27572, CVE-2025-27940, CVE-2026-35071, CVE-2026-40638, CVE-2026-26945, CVE-2026-26948)
Description	Dell 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. 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/000455614/dsa-2026-198 • https://www.dell.com/support/kbdoc/en-us/000458101/dsa-2026-205 • https://www.dell.com/support/kbdoc/en-us/000438301/dsa-2026-128 • https://www.dell.com/support/kbdoc/en-us/000463695/dsa-2026-208-security-update-for-dell-powerscale-insightiq-multiple-vulnerabilities

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23411, CVE-2026-23410, CVE-2026-23405, CVE-2026-23404, CVE-2026-23403, CVE-2026-23269, CVE-2026-23268, CVE-2026-23209, CVE-2026-23074, CVE-2026-23060, CVE-2025-37849, CVE-2025-21735, CVE-2024-50142, CVE-2024-50008, CVE-2024-49938, CVE-2024-46816, CVE-2024-46777, CVE-2024-27388)
Description	Ubuntu 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 Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu versions: • 18.04 LTS • 16.04 LTS • 20.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8267-1 • https://ubuntu.com/security/notices/USN-8266-1 • https://ubuntu.com/security/notices/USN-8255-2

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
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 systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Cloud Pak for Data System – Cyclops IBM HTTP Server version 8.5 and 9.0 API Connect V12 OnPrem version 12.1.0.0 to 12.1.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7272521 • https://www.ibm.com/support/pages/node/7272621 • https://www.ibm.com/support/pages/node/7272626

Affected Product	**QNAP**
Severity	**Medium**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2026-43284)
Description	QNAP has released a security update addressing a vulnerability that exists in their products. **CVE-2026-43284**: A local privilege escalation vulnerability, colloquially known as "Dirty Frag" (CVE-2026-43284), has been reported to affect the Linux kernel. If exploited, this vulnerability allows an authenticated local user with standard privileges to bypass security restrictions and gain elevated system (root) permissions. QNAP advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	All QNAP x86-based NAS models All QNAP ARM64-based NAS models All QuTS hero NAS models All QuTScloud NAS instances
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-26-17

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.