Advisory Alert

Alert Number: AAA20250716 **Date:** July 16, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Node.js	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
Dell	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52933, CVE-2025-21759, CVE-2025-22004, CVE-2025-22121, CVE-2025-23150, CVE-2025-37738, CVE-2025-38110)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause use after free, out-of-bound read, out-of-bound write. 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 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:11245

Affected Product	**Node.js**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-27210, CVE-2025-27209)
Description	Nodejs has released security updates addressing multiple vulnerabilities that exist in Their products. **CVE-2025-27210** - An incomplete fix has been identified for CVE-2025-23084 in Node.js, specifically affecting Windows device names like CON, PRN, and AUX. **CVE-2025-27209** - The V8 release used in Node.js v24.0.0 has changed how string hashes are computed using rapidhash. This implementation re-introduces the HashDoS vulnerability as an attacker who can control the strings to be hashed can generate many hash collisions - an attacker can generate collisions even without knowing the hash-seed. Nodejs advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Node.js versions prior to - 24.x, 22.x, 20.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nodejs.org/en/blog/vulnerability/july-2025-security-releases

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause use after free, out-of-bound read, memory accesses, limit validation. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.5 SUSE Linux Enterprise Micro 5.1 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Micro for Rancher 5.3 SUSE Linux Enterprise Micro for Rancher 5.4 SUSE Linux Enterprise Server 11 SP4 SUSE Linux Enterprise Server 11 SP4 LTSS EXTREME CORE
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202502312-1 • https://www.suse.com/support/update/announcement/2025/suse-su-202502320-1 • https://www.suse.com/support/update/announcement/2025/suse-su-202502321-1 • https://www.suse.com/support/update/announcement/2025/suse-su-202502322-1

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-33097, CVE-2023-33953, CVE-2023-44487, CVE-2023-32732, CVE-2022-49395, CVE-2024-52005, CVE-2025-22869, CVE-2025-5283, CVE-2025-48976, CVE-2025-48988, CVE-2025-49125, CVE-2020-16156, CVE-2025-21587, CVE-2025-30698, CVE-2025-4447, CVE-2025-32414, CVE-2025-48734)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause cross-site scripting, use after free, improper access control, buffer overflow. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM Versions - 7.5 - 7.5.0 UP12 IF02
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7239755 • https://www.ibm.com/support/pages/node/7239753 • https://www.ibm.com/support/pages/node/7239757

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-36603, CVE-2025-32744)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-36603** - Dell AppSync, version(s) 4.6.0.0, contains an Improper Restriction of XML External Entity Reference vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure and Information tampering. **CVE-2025-32744** - Dell AppSync, version(s) 4.6.0.0, contains an Unrestricted Upload of File with Dangerous Type vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Remote execution. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell AppSync Versions prior to - 4.6.0.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000345331/dsa-2025-277-security-update-for-dell-appsync-vulnerabilities

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.