Advisory Alert

Alert Number: **AAA20251127** **Date:** **November 27, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Red Hat	**Medium**	Improper Restriction of XML External Entity Reference Vulnerability

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53141, CVE-2025-23145, CVE-2024-53141, CVE-2025-23145, CVE-2025-38500, CVE-2025-38616)
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 this security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20254255-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254256-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254261-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254262-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254265-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254268-1/

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-57699, CVE-2025-7962)
Description	IBM has released security updates addressing vulnerabilities that exist in their products. **CVE-2024-57699**: When loading a specially crafted JSON input, containing a large number of ’{’, a stack exhaustion can be trigger, which could allow an attacker to cause a Denial of Service (DoS). This issue exists because of an incomplete fix for CVE-2023-1370. **CVE-2025-7962**: In Jakarta Mail 2.0.2 it is possible to perform a SMTP Injection by utilizing the \r and \n UTF-8 characters to separate different messages. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Db2 Server versions: • 11.1.0 - 11.1.4.7 • 11.5.0 - 11.5.9 • 12.1.0 - 12.1.3 IBM WebSphere Remote Server versions 8.5, 9.0, 9.1 WebSphere Service Registry and Repository versions 8.5 to 8.5.6.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7250474 • https://www.ibm.com/support/pages/node/7252838 • https://www.ibm.com/support/pages/node/7252718

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-0395, CVE-2025-0690, CVE-2025-1125, CVE-2025-0689, CVE-2025-0686, CVE-2025-0624, CVE-2025-0622, CVE-2025-0677, CVE-2025-1118, CVE-2024-56737, CVE-2025-0678, CVE-2025-0725, CVE-2025-0167, CVE-2025-24928, CVE-2025-26465, CVE-2021-28041)
Description	Dell has released a security update addressing multiple third-party vulnerabilities that exist in NetWorker vProxy. These vulnerabilities could be exploited by malicious users to conduct Buffer Overflow, Machine-in-the-Middle, and Information Leakage. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	NetWorker vProxy versions, • 19.12 through 19.12.0.1 • prior to 19.11.0.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000337955/dsa-2025-262-security-update-for-dell-networker-vproxy-multiple-third-party-component-vulnerabilities

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Improper Restriction of XML External Entity Reference Vulnerability (CVE-2025-4949)
Description	Red Hat has released security updates addressing an XML External Entity (XXE) vulnerability that exists in their products. This vulnerability could be exploited by malicious users to compromise the affected systems. Red Hat advises to apply this security fix at your earliest to protect your systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 8.1 for RHEL 9 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:22188 • https://access.redhat.com/errata/RHSA-2025:22190

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.