TLP: WHITE

Advisory Alert

Alert Number: AAA20251202 **Date:** December 2, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Apache Struts 2	**High**	Information Disclosure Vulnerability
Dell	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Red Hat	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-42516, CVE-2024-43204, CVE-2024-43394, CVE-2024-47252, CVE-2025-23048, CVE-2025-48976, CVE-2025-48988, CVE-2025-48989, CVE-2025-49124, CVE-2025-49125, CVE-2025-49630, CVE-2025-49812, CVE-2025-52520, CVE-2025-53020, CVE-2025-53506, CVE-2025-54090)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell NetWorker Software. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell NetWorker Management Console and NetWorker Management Web UI Versions prior to 19.13.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000397532/dsa-2025-365-security-update-for-dell-networker-multiple-third-party-component-vulnerabilities

Affected Product	**Apache Struts 2**
Severity	**High**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2025-64775)
Description	The ASF has released security updates addressing a file leak in multipart request processing which causes disk exhaustion (DoS) in Struts 2. ASF advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Struts 6.0.0 through Struts 6.7.0 Struts 7.0.0 through Struts 7.0.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://cwiki.apache.org/confluence/display/WW/S2-068

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-24189, CVE-2025-31257, CVE-2025-31273, CVE-2025-31278, CVE-2025-43211, CVE-2025-43212, CVE-2025-43216, CVE-2025-43227, CVE-2025-43228, CVE-2025-43240, CVE-2025-43265, CVE-2025-6558, CVE-2025-53057, CVE-2025-53066, CVE-2025-61755)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell NetWorker Runtime Environment. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell NetWorker Runtime Environment (NRE) Version 17.0.2 and 8.0.26
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000397455/dsa-2025-438-security-update-for-dell-networker-runtime-environment-multiple-third-party-component-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-50116, CVE-2022-50252, CVE-2022-50272, CVE-2022-50381, CVE-2022-50409, CVE-2023-28328, CVE-2023-3772, CVE-2023-53147, CVE-2023-53282, CVE-2023-53322, CVE-2023-53365, CVE-2023-53395, CVE-2023-53705, CVE-2023-53722, CVE-2025-38352, CVE-2025-38498, CVE-2025-38616, CVE-2025-38617, CVE-2025-38685, CVE-2025-38713, CVE-2025-39973)
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 system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise Server 11 SP4 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server 11 SP4 LTSS EXTREME CORE SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Real Time 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/2025/suse-su-20254315-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254311-1/

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-53513, CVE-2025-38724, CVE-2025-39825, CVE-2025-39864, CVE-2025-39881, CVE-2025-39883, CVE-2025-39898, CVE-2025-39918, CVE-2025-39955, CVE-2025-39981, CVE-2025-40058, CVE-2025-40185, CVE-2025-40186)
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 system. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat CodeReady Linux Builder for ARM 64 8 aarch64, 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le, 9 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64, 9 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 8 aarch64, 9 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for IBM z Systems 8 s390x, 9 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for Power, little endian 8 ppc64le, 9 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64, 9 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:22392 • https://access.redhat.com/errata/RHSA-2025:22388 • https://access.redhat.com/errata/RHSA-2025:22405

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.