Advisory Alert

Alert Number: AAA20260202 **Date:** February 2, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Ubuntu	**High**, Medium	Multiple Vulnerabilities
IBM	Medium	Authentication Bypass vulnerability
Red Hat	Medium	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Networker vProxy Versions 19.8 - 19.13.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000421570/dsa-2026-030-security-update-for-dell-networker-vproxy-multiple-third-party-component-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-23559, CVE-2023-54110, CVE-2023-54168, CVE-2025-40018 , CVE-2025-40215)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. 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 11 SP4 LTSS EXTREME CORE
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20260352-1/

Affected Product	**Ubuntu**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40019, CVE-2025-21726, CVE-2022-49698)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-40019 -** A Linux kernel vulnerability in the crypto ESSIV implementation, where ssize (signed size) checks were incorrectly handled during decryption and in-place encryption. This could lead to inconsistent cryptographic behavior or crashes if the check isn't applied at the correct stage of the ESSIV routine. **CVE-2025-21726** - A use-after-free flaw in the Linux kernel's padata subsystem affecting the reorder_work functionality, where improper reference handling can cause freed memory to be accessed, potentially enabling local attackers to crash the system or escalate privileges. **CVE-2022-49698** - A vulnerability in the Linux kernel netfilter component where unsafe use of the pseudo-random generator (prandom) during per-CPU state updates can lead to race conditions, affecting network packet filtering and potentially causing instability or information leaks. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu Versions 20.04 and 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7990-1

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Authentication Bypass vulnerability (CVE-2025-36365)
Description	IBM has released security updates addressing a vulnerability that exists in their Db2 Server products. **CVE-2025-36365**– An Authentication Bypass vulnerability where under specific configuration of cataloged remote storage aliases could allow an authenticated user to execute unauthorized commands using a user-controlled key. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 versions 11.5.0 - 11.5.9 and 12.1.0 - 12.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7257665

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38568, CVE-2025-40154, CVE-2025-40251)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the kernel component of their products. **CVE-2025-38568** - A Linux kernel vulnerability in the net/sched mqprio subsystem where improper validation of the mqprio traffic class entry index leads to a stack out-of-bounds write, potentially resulting in memory corruption or instability when parsing traffic control entries. **CVE-2025-40154** - An issue in the Linux kernel's ASoC Intel bytcr_rt5640 driver involving invalid quirk input mapping, which could lead to unexpected behavior such as out-of-bounds access; the patch corrects the input interpretation logic. **CVE-2025-40251** - A Linux kernel vulnerability in the devlink rate handling code where failing to clear the parent pointer in devl_rate_nodes_destroy leaves a dangling pointer, risking refcount errors and related instability in network device subsystems. 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 9 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:1617

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.