



Advisory Alert

Alert Number: AAA20251107 Date: November 7, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	Critical	Stack-based Buffer Overflow Vulnerability
SUSE	High	Null Pointer Dereference Vulnerability
Dell	High, Medium	Multiple Vulnerabilities
Red Hat	High, Medium	Multiple Vulnerabilities
Ubuntu	High, Medium	Multiple Vulnerabilities
IBM	High, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	IBM
Severity	Critical
Affected Vulnerability	Stack-based Buffer Overflow Vulnerability (CVE-2025-30472)
Description	<p>IBM has released a security update addressing a Stack-based Buffer Overflow vulnerability that exists in IBM Db2.</p> <p>CVE-2025-30472 - Corosync through 3.1.9, if encryption is disabled or the attacker knows the encryption key, has a stack-based buffer overflow in orf_token_endian_convert in exec/totemsrp.c via a large UDP packet.</p> <p>IBM advises to apply this security fix at your earliest to protect your systems from potential threats.</p>
Affected Products	IBM Db2 Server 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/7240977

Affected Product	SUSE
Severity	High
Affected Vulnerability	Null Pointer Dereference Vulnerability (CVE-2025-38664)
Description	<p>SUSE has released a security update addressing a Null Pointer Dereference vulnerability that exists in their products.</p> <p>CVE-2025-38664: ice: Fix a null pointer dereference in ice_copy_and_init_pkg()</p> <p>SUSE advises to apply this security fix at your earliest to protect your systems from potential threats.</p>
Affected Products	openSUSE Leap 15.6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2025/suse-su-20253970-1/

Affected Product	Dell
Severity	High, Medium
Affected Vulnerability	Multiple Vulnerabilities
Description	<p>Dell has released security updates addressing a multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems.</p> <p>Dell advises to apply this security fixes at your earliest to protect your systems from potential threats.</p>
Affected Products	Dell Enterprise SONiC Distribution Versions prior to 4.5.1 iDRAC9 Versions prior to 7.00.00.181, and 6.10.80.00 to 7.20.10.50 iDRAC10 Versions prior to 1.20.25.00
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<ul style="list-style-type: none">https://www.dell.com/support/kbdoc/en-us/000388143/https://www.dell.com/support/kbdoc/en-us/000384516/

TLP: WHITE

Affected Product	Red Hat
Severity	High, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-31651, CVE-2025-55752, CVE-2022-50367, CVE-2023-53178, CVE-2023-53331, CVE-2023-53401, CVE-2024-46679, CVE-2025-39730)
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	JBoss Enterprise Web Server 6 for RHEL 10 x86_64 JBoss Enterprise Web Server 6 for RHEL 9 x86_64 JBoss Enterprise Web Server 6 for RHEL 8 x86_64 JBoss Enterprise Web Server Text-Only Advisories x86_64 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	<ul style="list-style-type: none">https://access.redhat.com/errata/RHSA-2025:19809https://access.redhat.com/errata/RHSA-2025:19810https://access.redhat.com/errata/RHSA-2025:19886

Affected Product	Ubuntu
Severity	High, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40300, CVE-2025-38352, CVE-2025-38118, CVE-2025-37838, CVE-2024-56767, CVE-2024-53150, CVE-2024-53124, CVE-2024-50299, CVE-2024-50006, CVE-2023-52650, CVE-2023-52574, CVE-2021-47330, CVE-2021-47294)
Description	Ubuntu has released security updates addressing a 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 fix at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu <ul style="list-style-type: none">Version 25.04Version 24.04Version 22.04Version 20.04Version 16.04Version 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<ul style="list-style-type: none">https://ubuntu.com/security/notices/USN-7860-1https://ubuntu.com/security/notices/USN-7861-1https://ubuntu.com/security/notices/USN-7862-1https://ubuntu.com/security/notices/USN-7863-1

Affected Product	IBM
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21587, CVE-2025-30698, CVE-2025-4447, CVE-2021-23445)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to conduct Unauthorized Access, Buffer Overflow and Cross Site Scripting. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Storage Protect for Space Management version 8.1.27 IBM Storage Protect for Virtual Environments: Data Protection for Hyper-V version 8.1.27 IBM Storage Protect Client version 8.1.27 IBM Storage Protect for Virtual Environments: Data Protection for VMware version 8.1.27 IBM Storage Scale versions 5.2.3.0 to 5.2.3.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<ul style="list-style-type: none">https://www.ibm.com/support/pages/node/7250253https://www.ibm.com/support/pages/node/7250083

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.