Advisory Alert

Alert Number: AAA20260213 **Date:** February 13, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
PostgreSQL	**High**, Medium	Multiple Vulnerabilities
HPE	**High**, Medium, Low	Multiple Vulnerabilities
Red Hat	Medium	Multiple Vulnerabilities
Ubuntu	Medium	Multiple Vulnerabilities

Description

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 compromise affected systems. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Public Cloud Module 15-SP7 openSUSE Leap 15.6 SUSE Linux Enterprise High Availability Extension 15 SP6 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server 15 SP6 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP7 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 12 SP5 LTSS SUSE Linux Enterprise Server 12 SP5 LTSS Extended Security SUSE Linux Enterprise Server for SAP Applications 12 SP5 openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP5 SUSE Linux Enterprise High Performance Computing LTSS 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 15 SP5 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP5 openSUSE Leap 15.3 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Micro for Rancher 5.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2026/suse-su-20260475-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260474-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260473-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260472-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260471-1/

Affected Product	**PostgreSQL**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-2003, CVE-2026-2004, CVE-2026-2005, CVE-2026-2006, CVE-2026-2007)
Description	PostgreSQL has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. PostgreSQL advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PostgreSQL versions 18.1-18.0 and all versions prior to 18.2, 17.8, 16.12, 15.16, and 14.21
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.postgresql.org/about/news/postgresql-182-178-1612-1516-and-1421-released-3235/

Affected Product	**HPE**
Severity	**High**, **Medium**, **low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-22853, CVE-2025-21096, CVE-2025-20067, CVE-2025-22392, CVE-2025-20053, CVE-2025-24305, CVE-2025-21090)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE SimpliVity 380 Gen11 - Prior to SimpliVity Support Pack Gen11 (SVTSPGen11) 2026_0116 HPE SimpliVity 380 Gen10 Plus - Prior to SimpliVity Support Pack Gen10 (SVTSPGen10) 2026_0116
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04938en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04937en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04939en_us&docLocale=en_US

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-50341, CVE-2022-50673, CVE-2023-53539, CVE-2023-53581, CVE-2023-53833, CVE-2025-40154, CVE-2025-40304, CVE-2025-40322, CVE-2025-68301, CVE-2025-68349)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the kernel of their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - AUS 8.2 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:2664

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in the kernel of their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu versions 25.10, 22.04, and 20.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8029-1 • https://ubuntu.com/security/notices/USN-8033-1 • https://ubuntu.com/security/notices/USN-8033-2

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.