Advisory Alert

Alert Number: AAA20260311 **Date:** March 11, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SAP	**Critical**	Multiple Vulnerabilities
HPE	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
Ivanti	**High**	Privilege Escalation Vulnerability
Dell	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
WordPress	**High**	Multiple Vulnerabilities
Lenovo	**High**, Medium	Multiple Vulnerabilities
Intel	**High**, Medium	Multiple Vulnerabilities
Fortinet	**High**, Medium, Low	Multiple Vulnerabilities
SAP	**High**, Medium, Low	Multiple Vulnerabilities
Red Hat	Medium	Multiple Vulnerabilities

Description

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2019-17571, CVE-2026-27685)
Description	SAP has released monthly security updates addressing multiple vulnerabilities that exist in their Products. **CVE-2019-17571**- Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data. This affects Log4j versions up to 1.2 up to 1.2.17. **CVE-2026-27685**- SAP NetWeaver Enterprise Portal Administration is vulnerable if a privileged user uploads untrusted or malicious content that, upon deserialization, could result in a high impact on the confidentiality, integrity, and availability of the host system. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SAP Quotation Management Insurance application (FS-QUO) Version(s) - FS-QUO 800 SAP NetWeaver Enterprise Portal Administration Version(s) - EP-RUNTIME 7.50
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/march-2026.html

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-22850, CVE-2025-22444, CVE-2025-20064, CVE-2025-20068, CVE-2025-20105, CVE-2025-20028, CVE-2025-20027, CVE-2025-20073, CVE-2026-23813, CVE-2026-23814, CVE-2026-23815, CVE-2026-23816, CVE-2026-23817)
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 Aruba Networking AOS-CX Software Version(s):** • AOS-CX 10.17.xxxx: 10.17.0001 and prior • AOS-CX 10.16.xxxx: 10.16.1020 and prior • AOS-CX 10.13.xxxx: 10.13.1160 and prior • AOS-CX 10.10.xxxx: 10.10.1170 and prior **HPE Gen12 Series** • HPE ProLiant Compute (DL320, DL340, DL360, DL380, DL380a, DL580, ML350, XD230): Prior to 1.40_05-22-2025 **HPE Gen11 Series** • HPE Alletra (4110, 4120, 4140): Prior to 2.60_08-07-2025 • HPE ProLiant (DL110, DL320, DL360, DL380, DL380a, DL560, ML110, ML350): Prior to 2.60_08-07-2025 • HPE Synergy 480 / Compute Edge e930t: Prior to 2.60_08-07-2025 • HPE ProLiant (DL20, ML30, MicroServer): Prior to 2.30_08-06-2025 **HPE Gen10 Plus Series** • HPE ProLiant (DL20, DL110, DL360, DL380, ML30, XL220n, XL290n, XL420, MicroServer v2): Prior to 2.50_08-06-2025 • HPE Edgeline (e920, e920d, e920t) / Apollo (2000, 4200) / Synergy 480: Prior to 2.50_08-06-2025 **HPE Gen10 Series** • HPE ProLiant (DL160, DL180, DL360, DL380, DL560, DL580, ML110, ML350, e910, e910t): Prior to 3.60_08-06-2025 • HPE Apollo (4200, XL420): Prior to 3.60_08-06-2025 HPE ProLiant (DL20, ML30, MicroServer, m750 Server Blade): Prior to 3.70_08-06-2025

Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05027en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05028en_us&docLocale=en_US

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Microsoft has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Microsoft advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Microsoft Office LTSC for Mac 2024 Microsoft Office LTSC 2024 for 64-bit editions Microsoft Office LTSC 2024 for 32-bit editions Microsoft Office LTSC 2021 for 32-bit editions Microsoft Office LTSC 2021 for 64-bit editions Windows Server 2025 Windows 11 Version 24H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows Server 2022, 23H2 Edition (Server Core installation) Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 11 Version 25H2 for x64-based Systems Windows 11 Version 25H2 for ARM64-based Systems Windows Server 2025 (Server Core installation) Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows Server 2022 (Server Core installation) Windows Server 2022 Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 11 version 26H1 for x64-based Systems Windows 11 Version 26H1 for ARM64-based Systems Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 Windows Server 2016 (Server Core installation) Windows Server 2016 Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows Server 2012 (Server Core installation) Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft 365 Apps for Enterprise for 64-bit Systems Azure Automation Hybrid Worker Windows Extension ASP.NET Core 10.0 ASP.NET Core 9.0 ASP.NET Core 8.0 Microsoft Authenticator for IOS Microsoft Authenticator for Android Azure MCP Server Tools Arc Enabled Servers - Azure Connected Machine Agent Microsoft Office for Android Microsoft Office 2016 (64-bit edition) Microsoft Office 2016 (32-bit edition) Microsoft Office LTSC for Mac 2021 Microsoft Office 2019 for 64-bit editions Microsoft Office 2019 for 32-bit editions Microsoft Excel 2016 (64-bit edition) Microsoft Excel 2016 (32-bit edition) Office Online Server Microsoft SharePoint Server Subscription Edition Microsoft SharePoint Server 2019 Microsoft SharePoint Enterprise Server 2016 Azure Linux Virtual Machines with Azure Diagnostics extension Azure IoT Explorer GitHub Repo: Zero Shot scFoundation Microsoft Azure AD SSH Login extension for Linux Microsoft.Bcl.Memory 9.0 .NET 9.0 installed on Windows .NET 9.0 installed on Mac OS .NET 9.0 installed on Linux .NET 10.0 installed on Linux .NET 10.0 installed on Mac OS .NET 10.0 installed on Windows Microsoft.Bcl.Memory 10.0 Microsoft SQL Server 2025 for x64-based Systems (CU2) Microsoft SQL Server 2025 for x64-based Systems (GDR) Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 Azure Connect Feature Pack Microsoft SQL Server 2019 for x64-based Systems (GDR) Microsoft SQL Server 2022 for x64-based Systems (CU 23) Microsoft SQL Server 2019 for x64-based Systems (CU 32) Microsoft SQL Server 2022 for x64-based Systems (GDR) Microsoft SQL Server 2017 for x64-based Systems (CU 31) Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR) Microsoft SQL Server 2017 for x64-based Systems (GDR) System Center Operations Manager 2025 System Center Operations Manager 2022 System Center Operations Manager 2019 Windows App Client for Windows Desktop Windows Admin Center in Azure Portal Windows Admin Center Microsoft Edge (Chromium-based)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2026-3483)
Description	Ivanti has released security updates addressing a vulnerability that exist in their products. **CVE-2026-3483 -** An exposed dangerous method in Ivanti DSM before version 2026.1.1 allows a local authenticated attacker to escalate their privileges. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Desktop and Server Management (DSM) • DSM 2026.1 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-DSM-CVE-2026-3483?language=en_US

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-12680, CVE-2025-12679, CVE-2025-12772, CVE-2025-12773, CVE-2025-12774, CVE-2025-21991, CVE-2024-3661, CVE-2024-11187, CVE-2024-12797, CVE-2025-26465, CVE-2025-32728, CVE-2023-25194, CVE-2025-27819, CVE-2025-27818, CVE-2022-34917, CVE-2024-31141, CVE-2024-56128, CVE-2025-4207)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in the third party components of 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	Connectrix B-Series Hardware Connectrix B-Series Software Connectrix DS-6520B Connectrix DS 300B Connectrix DS 6505B Connectrix DS 6510B Connectrix DS 6610B Connectrix DS 6620B Connectrix DS 6630B Connectrix SANnav Avamar Avamar Data Store Avamar Data Store Gen5A Avamar Server
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000437875/dsa-2026-088-security-update-for-dell-connectrix-b-series-sannav-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000437867/dsa-2026-087-security-update-for-dell-connectrix-b-series-fos-and-sannav-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000437829/dsa-2026-086-security-update-for-dell-avamar-data-store-gen5a-multiple-third-party-component-vulnerabilities

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-22850, CVE-2025-22444, CVE-2025-20064, CVE-2025-20068, CVE-2025-20105, CVE-2025-20028, CVE-2025-20027, CVE-2025-20073, CVE-2026-23813, CVE-2026-23814, CVE-2026-23815, CVE-2026-23816, CVE-2026-23817)
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 Aruba Networking AOS-CX Software Version(s):** • AOS-CX 10.17.xxxx: 10.17.0001 and prior • AOS-CX 10.16.xxxx: 10.16.1020 and prior • AOS-CX 10.13.xxxx: 10.13.1160 and prior • AOS-CX 10.10.xxxx: 10.10.1170 and prior **HPE Gen12 Series** • HPE ProLiant Compute (DL320, DL340, DL360, DL380, DL380a, DL580, ML350, XD230): Prior to 1.40_05-22-2025 **HPE Gen11 Series** • HPE Alletra (4110, 4120, 4140): Prior to 2.60_08-07-2025 • HPE ProLiant (DL110, DL320, DL360, DL380, DL380a, DL560, ML110, ML350): Prior to 2.60_08-07-2025 • HPE Synergy 480 / Compute Edge e930t: Prior to 2.60_08-07-2025 • HPE ProLiant (DL20, ML30, MicroServer): Prior to 2.30_08-06-2025 **HPE Gen10 Plus Series** • HPE ProLiant (DL20, DL110, DL360, DL380, ML30, XL220n, XL290n, XL420, MicroServer v2): Prior to 2.50_08-06-2025 • HPE Edgeline (e920, e920d, e920t) / Apollo (2000, 4200) / Synergy 480: Prior to 2.50_08-06-2025 **HPE Gen10 Series** • HPE ProLiant (DL160, DL180, DL360, DL380, DL560, DL580, ML110, ML350, e910, e910t): Prior to 3.60_08-06-2025 • HPE Apollo (4200, XL420): Prior to 3.60_08-06-2025 • HPE ProLiant (DL20, ML30, MicroServer, m750 Server Blade): Prior to 3.70_08-06-2025
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05027en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05028en_us&docLocale=en_US

Affected Product	**WordPress**
Severity	**High**
Affected Vulnerability	Security Update
Description	WordPress has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. WordPress advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WordPress versions prior to 6.9.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wordpress.org/news/2026/03/wordpress-6-9-2-release/

Affected Product	**Lenovo**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-1652, CVE-2026-1653, CVE-2026-20423, CVE-2026-20436, CVE-2025-25176, CVE-2025-58408, CVE-2025-58409, CVE-2026-20416, CVE-2026-20424, CVE-2026-20425, CVE-2026-20426, CVE-2026-20427, CVE-2026-20428, CVE-2026-20429, CVE-2026-20430, CVE-2026-20434, CVE-2026-20435, CVE-2026-20437, CVE-2026-20438, CVE-2026-20439, CVE-2026-20440, CVE-2026-20441, CVE-2026-20442, CVE-2026-20443, CVE-2026-20444, CVE-2026-20445, CVE-2025-20005, CVE-2025-20027, CVE-2025-20028, CVE-2025-20064, CVE-2025-20068, CVE-2025-20073, CVE-2025-20096, CVE-2025-20105, CVE-2025-22444, CVE-2025-22850, CVE-2026-0940, CVE-2026-1715, CVE-2026-1716, CVE-2026-1717)
Description	Lenovo has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Lenovo advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/us/en/product_security/LEN-213044 https://support.lenovo.com/us/en/product_security/LEN-213040 https://support.lenovo.com/us/en/product_security/LEN-210876 https://support.lenovo.com/us/en/product_security/LEN-210875 https://support.lenovo.com/us/en/product_security/LEN-209683

Affected Product	**Intel**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20105, CVE-2025-20064, CVE-2025-20028, CVE-2025-20068, CVE-2025-20027, CVE-2025-22850, CVE-2025-22444, CVE-2025-20005, CVE-2025-20073, CVE-2025-20096)
Description	Intel has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Intel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Intel Core Series • Intel Core Ultra Processors (Series 1 & 2) • Intel Core Processors (7th, 8th, 9th, 10th, 11th, 12th, & 13th Gen) • Intel Core X-series Processors / Family Intel Xeon Series • Intel Xeon 6 • Intel Xeon Scalable Processors (1st, 2nd, 3rd, 4th, & 5th Gen) • Intel Xeon W Processors (2100, 2200, 3100 series & Family) • Intel Xeon E Processors / Family • Intel Xeon D Processors / Family / NS Family • Intel Xeon Processor E7 v3 & E5 v4 Families Intel Atom Series • Intel Atom Processors / P6000 • Intel Atom Processor X Series • Intel Atom C / C5000 / P5000 Families
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01234.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01393.html

Affected Product	**Fortinet**
Severity	**High**, **Medium**, **low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-53608, CVE-2026-24640, CVE-2026-30897, CVE-2025-49784, CVE-2026-25972, CVE-2026-25689, CVE-2026-22629, CVE-2026-24017, CVE-2025-54820, CVE-2025-68648, CVE-2025-55717, CVE-2025-68482, CVE-2026-24018, CVE-2026-22572, CVE-2026-24641, CVE-2025-66178, CVE-2025-48418, CVE-2025-48840)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Fortinet advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-26-091 https://www.fortiguard.com/psirt/FG-IR-26-087 https://www.fortiguard.com/psirt/FG-IR-26-093 https://www.fortiguard.com/psirt/FG-IR-26-095 https://www.fortiguard.com/psirt/FG-IR-26-077 https://www.fortiguard.com/psirt/FG-IR-26-097 https://www.fortiguard.com/psirt/FG-IR-26-081 https://www.fortiguard.com/psirt/FG-IR-26-088 https://www.fortiguard.com/psirt/FG-IR-26-089 https://www.fortiguard.com/psirt/FG-IR-26-090 https://www.fortiguard.com/psirt/FG-IR-26-083 https://www.fortiguard.com/psirt/FG-IR-26-078 https://www.fortiguard.com/psirt/FG-IR-26-080 https://www.fortiguard.com/psirt/FG-IR-26-092 https://www.fortiguard.com/psirt/FG-IR-26-098 https://www.fortiguard.com/psirt/FG-IR-26-082 https://www.fortiguard.com/psirt/FG-IR-26-079 https://www.fortiguard.com/psirt/FG-IR-26-094

Affected Product	**SAP**
Severity	**High**, **Medium**, **low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-27689, CVE-2026-24316, CVE-2026-24309, CVE-2026-27684, CVE-2026-0489, CVE-2026-27686, CVE-2026-27687, CVE-2026-24311, CVE-2026-24317, CVE-2026-27688, CVE-2026-24313, CVE-2025-9230, CVE-2025-9232, CVE-2026-24310)
Description	SAP has released monthly security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	(Please refer to the provided referral link for specific product versions) SAP Supply Chain Management SAP NetWeaver (Feedback Notification) SAP Business One (Job Service) SAP Business Warehouse (Service API) SAP S/4HANA HCM Portugal and SAP ERP HCM Portugal SAP Customer Checkout 2.0 SAP GUI for Windows with active GuiXT SAP NetWeaver Application Server for ABAP SAP Solution Tools Plug-In (ST-PI) SAP NetWeaver AS Java (Adobe Document Services)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/march-2026.html

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-47727, CVE-2025-38024, CVE-2025-38129, CVE-2025-38206, CVE-2025-71085, CVE-2025-37882, CVE-2025-40269)
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 affected systems. 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 - Extended Update Support Extension 8.8 x86_64 Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 s390x 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	• https://access.redhat.com/errata/RHSA-2026:4246 • https://access.redhat.com/errata/RHSA-2026:4245 • https://access.redhat.com/errata/RHSA-2026:4243 • https://access.redhat.com/errata/RHSA-2026:4242

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.