Advisory Alert

Alert Number: AAA20250611 **Date:** June 11, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SAP	**Critical**	Missing Authorization Check Vulnerability
NetApp	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Ivanti	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
SolarWinds	**High**, Medium	Multiple Vulnerabilities
AMD	**High**, Medium	Multiple Vulnerabilities
Fortinet	**High**, Medium, Low	Multiple Vulnerabilities
NetApp	**High**, Medium, Low	Multiple Vulnerabilities
SAP	**High**, Medium, Low	Multiple Vulnerabilities
Intel	Medium	Out-of-bounds Read Vulnerability
Red Hat	Medium	Multiple Vulnerabilities
IBM	Low	Information Disclosure Vulnerability

Description

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Missing Authorization Check Vulnerability (CVE-2025-42989)
Description	SAP has released security updates for the month of June addressing a Missing Authorization Check Vulnerability that exists in SAP NetWeaver Application Server for ABAP. **CVE-2025-42989** - RFC inbound processing does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. On successful exploitation the attacker could critically impact both integrity and availability of the application. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SAP NetWeaver Application Server for ABAP Kernel Versions 7.89, 7.93, 9.14, 9.15
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/june-2025.html

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-37371, CVE-2024-22243, CVE-2024-22259)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-37371** - Multiple NetApp products incorporate Oracle MySQL Server. Multiple MySQL Server versions are susceptible vulnerabilities that allow attackers with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. **CVE-2024-22243** - Multiple NetApp products incorporate Spring Framework. Spring Framework versions 6.1.0 through 6.1.3, 6.0.0 through 6.0.16, 5.3.0 through 5.3.31 and older unsupported versions are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information or addition or modification of data. **CVE-2024-22259** - Multiple NetApp products incorporate Spring Framework. Spring Framework versions 6.1.0 prior to 6.1.5, 6.0.0 prior to 6.0.18, 5.3.0 prior to 5.3.33 and older unsupported versions are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information or addition or modification of data. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Active IQ Unified Manager for Microsoft Windows Active IQ Unified Manager for Linux Active IQ Unified Manager for VMware vSphere NetApp BlueXP OnCommand Workflow Automation SnapCenter
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20250124-0010 • https://security.netapp.com/advisory/ntap-20240524-0001 • https://security.netapp.com/advisory/ntap-20240524-0002

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-32717, CVE-2025-47163, CVE-2025-33057, CVE-2025-33053, CVE-2025-33052, CVE-2025-33075, CVE-2025-33068, CVE-2025-33063, CVE-2025-33061, CVE-2025-32724, CVE-2025-32720, CVE-2025-32716, CVE-2025-32715, CVE-2025-32713, CVE-2025-47977, CVE-2025-47968, CVE-2025-47233, CVE-2025-47027, CVE-2025-47176, CVE-2025-47175, CVE-2025-47173, CVE-2025-47172, CVE-2025-47171, CVE-2025-47170, CVE-2025-47169, CVE-2025-47168, CVE-2025-47167, CVE-2025-47166, CVE-2025-47165, CVE-2025-47164, CVE-2025-47163, CVE-2025-33070, CVE-2025-33069, CVE-2025-33068, CVE-2025-33056, CVE-2025-33053, CVE-2025-33051, CVE-2025-33050, CVE-2025-32728, CVE-2025-32706, CVE-2025-24069, CVE-2025-24068, CVE-2025-24064, CVE-2025-47962, CVE-2025-33071, CVE-2025-47954, CVE-2025-47953, CVE-2025-47162, CVE-2025-33067, CVE-2025-33066, CVE-2025-33065, CVE-2025-33063, CVE-2025-33062, CVE-2025-33060, CVE-2025-33059, CVE-2025-33058, CVE-2025-32721, CVE-2025-32719, CVE-2025-32718, CVE-2025-32714, CVE-2025-32712, CVE-2025-32710, CVE-2025-30399, CVE-2025-47960, CVE-2025-47957, CVE-2025-47966, CVE-2025-47965, CVE-2025-24194)
Description	Microsoft has released security updates for the month of June addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Remote Code Execution, Elevation of Privilege, Denial of Service, Security Feature Bypass and Information Disclosure. Microsoft advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	.NET 8.0 installed on Linux .NET 8.0 installed on Mac OS .NET 8.0 installed on Windows .NET 9.0 installed on Linux .NET 9.0 installed on Mac OS .NET 9.0 installed on Windows Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft AutoUpdate for Mac Microsoft Edge (Chromium-based) Microsoft Excel 2016 (32-bit edition) Microsoft Excel 2016 (64-bit edition) Microsoft Office 2016 (32-bit edition) Microsoft Office 2016 (64-bit edition) Microsoft Office 2019 for 32-bit editions Microsoft Office 2019 for 64-bit editions Microsoft Office for Android Microsoft Office LTSC 2021 for 32-bit editions Microsoft Office LTSC 2021 for 64-bit editions Microsoft Office LTSC 2024 for 32-bit editions Microsoft Office LTSC 2024 for 64-bit editions Microsoft Office LTSC for Mac 2021 Microsoft Office LTSC for Mac 2024 Microsoft Outlook 2016 (32-bit edition) Microsoft Outlook 2016 (64-bit edition) Microsoft PowerPoint 2016 (32-bit edition) Microsoft PowerPoint 2016 (64-bit edition) Microsoft SharePoint Enterprise Server 2016 Microsoft SharePoint Server 2019 Microsoft SharePoint Server Subscription Edition Microsoft Visual Studio 2022 version 17.10 Microsoft Visual Studio 2022 version 17.12 Microsoft Visual Studio 2022 version 17.14 Microsoft Visual Studio 2022 version 17.8 Microsoft Word 2016 (32-bit edition) Microsoft Word 2016 (64-bit edition) Nuance Digital Engagement Platform Office Online Server Power Automate for Desktop Remote Desktop client for Windows Desktop Windows 10 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems 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 11 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows 11 Version 24H2 for x64-based Systems Windows App Client for Windows Desktop Windows SDK Windows Security App Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2012, (Server Core installation) Windows Server 2012 R2, (Server Core installation) Windows Server 2016, (Server Core installation) Windows Server 2019, (Server Core installation) Windows Server 2022, (Server Core installation) Windows Server 2022, 23H2 Edition (Server Core installation) Windows Server 2025, (Server Core installation)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-49080, CVE-2024-49855, CVE-2024-57996, CVE-2024-58013)
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	openSUSE Leap 15.3, 15.5 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP3, 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP3, 15-SP5 SUSE Linux Enterprise Micro 5.1, 5.2, 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 12 SP5, 15 SP3, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP3, 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202501869-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501868-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501849-1/

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-6763, CVE-2024-8184, CVE-2025-36574, CVE-2025-36575, CVE-2025-36578, CVE-2025-36580, CVE-2025-36577, CVE-2025-36576, CVE-2024-36293, CVE-2024-38307, CVE-2024-30211, CVE-2024-26021, CVE-2023-43758, CVE-2023-34440, CVE-2024-24582, CVE-2024-29214, CVE-2024-39279, CVE-2024-31157, CVE-2024-28047, CVE-2024-39355, CVE-2025-2884)
Description	Dell 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. Dell 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.dell.com/support/kbdoc/en-us/000325679/dsa-2025-226 • https://www.dell.com/support/kbdoc/en-us/000239036/dsa-2025-005

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-5353, CVE- CVE-2025-22463, CVE-2025-22455)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in Security Advisory Ivanti Workspace Control. **CVE-2025-5353** - A hardcoded key in Ivanti Workspace Control before version 10.19.10.0 allows a local authenticated attacker to decrypt stored SQL credentials. **CVE-2025-22463** - A hardcoded key in Ivanti Workspace Control before version 10.19.10.0 allows a local authenticated attacker to decrypt the stored environment password. **CVE-2025-22455** - A hardcoded key in Ivanti Workspace Control before version 10.19.0.0 allows a local authenticated attacker to decrypt stored SQL credentials. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Workspace Control (IWC) versions 10.19.0.0 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Workspace-Control-CVE-2025-5353-CVE-CVE-2025-22463-CVE-2025-22455?language=en_US

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-28893, CVE-2023-0394, CVE-2024-26923, CVE-2025-4661, CVE-2025-4663, CVE-2025-2884, CVE-2023-20599)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Directory Traversal, Arbitrary Code Execution and Unauthorized Access. HPE 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.hpe.com/hpesc/public/docDisplay?docId=hpesbst04879en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04874en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04882en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04880en_us&docLocale=en_US

Affected Product	**SolarWinds**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-26395, CVE-2025-26394)
Description	SolarWinds has released security updates addressing multiple vulnerabilities that exist in SolarWinds SWOSH. **CVE-2025-26395** - SolarWinds SWOSH was susceptible to a cross-site scripting (XSS) vulnerability due to an unsanitized field in the URL. The attack requires authentication using an administrator-level account and user interaction is required. **CVE-2025-26394** - SolarWinds SWOSH is susceptible to an open redirection vulnerability. The URL is not properly sanitized, and an attacker could manipulate the string to redirect a user to a malicious site. The attack complexity is high, and authentication is required. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds SWOSH 2025.1.1 and prior versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.solarwinds.com/trust-center/security-advisories/cve-2025-26395 • https://www.solarwinds.com/trust-center/security-advisories/cve-2025-26394

Affected Product	**AMD**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20599, CVE-2025-2884)
Description	AMD has released security updates addressing multiple vulnerabilities that exist in various AMD processors. **CVE-2023-20599** - Improper register access control in ASP may allow a privileged attacker to perform unauthorized access to ASP's Crypto Co-Processor (CCP) registers from x86, resulting in potential loss of control of cryptographic key pointer/index, leading to loss of integrity or confidentiality. **CVE-2025-2884** - An out-of-bounds read vulnerability exists in TPM2.0's Module Library allowing a read past the end of a TPM2.0 routine as described above. An attacker who can successfully exploit this vulnerability can read sensitive data stored in the TPM and/or impact the availability of the TPM. AMD 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.amd.com/en/resources/product-security/bulletin/amd-sb-7039.html • https://www.amd.com/en/resources/product-security/bulletin/amd-sb-4011.html

Affected Product	**Fortinet**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-48786, CVE-2025-22251, CVE-2024-54019, CVE-2025-25250, CVE-2024-45329, CVE-2024-50562, CVE-2025-31104, CVE-2023-42788, CVE-2025-22254, CVE-2025-22862, CVE-2023-29184, CVE-2024-32119, CVE-2024-50568, CVE-2025-24471)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Unauthorized Code or Commands Execution, DNS Spoofing, Information Disclosure. 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

Affected Product	**NetApp**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	NetApp 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. NetApp 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://security.netapp.com/advisory/

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-42982, CVE-2025-42983, CVE-2025-23192, CVE-2025-42977, CVE-2025-42994, CVE-2025-42995, CVE-2025-42996, CVE-2025-42993, CVE-2025-31325, CVE-2025-42984, CVE-2025-42998, CVE-2025-42987, CVE-2025-42991, CVE-2025-42988, CVE-2025-42990)
Description	SAP has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Information Disclosure, Cross-Site Scripting, Directory Traversal, Server-Side Request Forgery. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP GRC (AC Plugin) Versions - GRCPINW V1100_700, V1100_731 • SAP Business Warehouse and SAP Plug-In Basis Versions - PI_BASIS 2006_1_700, 701, 702, 731, 740, SAP_BW 750, 751, 752, 753, 754, 755, 756, 757, 758, 914, 915 • SAP BusinessObjects Business Intelligence (BI Workspace) Versions - ENTERPRISE 430, 2025, 2027 • SAP Business Objects Business Intelligence Platform Versions - ENTERPRISE 430, 2025, 2027 • SAP Business One Integration Framework Versions - B1_ON_HANA 10.0, SAP-M-BO 10.0 • SAP NetWeaver Visual Composer Version - VCBASE 7.50 • SAP NetWeaver (ABAP Keyword Documentation) Version - SAP_BASIS 758 • SAP MDM Server Versions - MDM_SERVER 710.750 • SAP S/4HANA (Enterprise Event Enablement) Versions - SAP_GWFND 757, 758 • SAP S/4HANA (Manage Central Purchase Contract application) Versions - S4CORE 106, 107, 108 • SAP S/4HANA (Manage Processing Rules - For Bank Statement) Versions - S4CORE 104, 105, 106, 107, 108 • SAP S/4HANA (Bank Account Application) Version - S4CORE 108 • SAPUI5 applications Versions - SAP_UI 750, 754, 755, 756, 757, 758, UI_700 200
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/june-2025.html

Affected Product	**Intel**
Severity	**Medium**
Affected Vulnerability	Out-of-bounds Read Vulnerability (CVE-2025-2884)
Description	Intel has released security updates addressing an Out-of-bounds Read Vulnerability that exists in Intel PTT and Intel SPS firmware. **CVE-2025-2884** - Out-of-bounds read in the firmware for some Intel PTT and Intel SPS may allow an authenticated user to potentially enable denial of service via local access. Intel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Intel® C420 Chipset 11.12.97 Intel® X299 Chipset11.12.97 Intel® C620 series chipset 11.22.97 8th Gen Intel® Core™ processor 11.8.97 Intel® 200 Series Chipset 11.8.97 Intel® 100 Series Chipset 11.8.97 8th Gen Intel® Core™ processor 12.0.96 Intel® 300 Series Chipset 12.0.96 Intel® C240 Series Chipset 12.0.96 Pentium® Gold processor series (G54XXU) Celeron® processor 4000 series (G54XXU) 10th Gen Intel® Core™ processor 13.0.70 Pentium® Silver processor series 13.50.30 Celeron® processor N series 13.50.30 Intel® 400 Series Chipset 14.1.75 Intel® 400 Series Chipset 14.5.55 Intel® 500 Series Chipset 15.0.50 Intel® C250 Series Chipset 15.0.50 Intel® C740 series chipset 15.20.20 Intel Atom® x6000E series 15.40.35 Intel Pentium® and Celeron® N and J Series processors 15.40.35 Intel® 600 Series Chipset 16.1.35 Intel® 700 series chipset 16.1.35 Intel® W790 chipset 16.11.20 Intel® 600 series chipset 16.50.15 Intel® Core™Ultra 18.0.10 Intel Atom® processor X E3900 series 3.1.97 Intel® Pentium® processor J4000/N4000 series 3.1.97 Celeron® processor J3000/N3000 series 3.1.97 Intel® Pentium® processor J5000/N5000 series 4.0.55 Celeron® processor J4000/N4000 series 4.0.55 Intel® C620A series chipset SPS_E5_04.04.04.701.0 Intel® C240 series chipset SPS_E3_05.01.05.003.0 Intel Atom® processor P5000 seriesSPS_SoC-A_05.00.03.404.0 Intel® Xeon® D processor 2000 series SPS_SoC-X_04.00.05.902.0 Intel® C620 series chipset SPS_E5_04.01.05.103.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01209.html

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-49395, CVE-2023-52606, CVE-2024-26645, CVE-2024-26921, CVE-2024-27042, CVE-2024-35930, CVE-2024-36933)
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 9.4 aarch64 Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:8796 • https://access.redhat.com/errata/RHSA-2025:8743

Affected Product	**IBM**
Severity	**Low**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2024-23454)
Description	IBM has released security updates addressing an Information Disclosure Vulnerability that exist in a third party product that affects IBM Db2 Server running on Linux. **CVE-2024-23454** - Apache Hadoop could allow a local authenticated attacker to obtain sensitive information, caused by not set permissions for temporary directory by default in the RunJar.run() function. By sending a specially crafted request, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Server running on Linux 11.1.0 - 11.1.4.7, 11.5.0 - 11.5.9 and 12.1.0 - 12.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7235070

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.