Advisory Alert

Alert Number: AAA20250909 **Date:** September 9, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SAP	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Security Update
Red Hat	**High**	Multiple Vulnerabilities
NetApp	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
HPE	**High**, **Medium**	Multiple Vulnerabilities
Dell	**High**, **Medium**	Multiple Vulnerabilities
SAP	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-42944, CVE-2025-42922, CVE-2023-27500, CVE-2025-42958)
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 the affected system. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP NetWeaver (RMI-P4) Version - SERVERCORE 7.50 • SAP NetWeaver AS Java (Deploy Web Service) Version - J2EE-APPS 7.50 • SAP NetWeaver AS for ABAP and ABAP Platform Version – 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757 • SAP NetWeaver Version - KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, KERNEL 7.22, 7.53, 7.54
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/september-2025.html

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2024-52316, CVE-2024-52317, CVE-2024-52318, CVE-2024-54677, CVE-2025-31650, CVE-2025-31651, CVE-2025-46701)
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 Management Web UI Versions - prior to 19.13.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000362754/dsa-2025-309-security-update-for-dell-networker-apache-tomcat-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-49985, CVE-2025-38352, CVE-2025-22097, CVE-2025-37803, CVE-2025-38350, CVE-2025-38449)
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 Enterprise Linux for Real Time 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 Red Hat Enterprise Linux for x86_64 10 x86_64 - Extended Update Support 10.0 x86_64 Red Hat Enterprise Linux for IBM z Systems 10 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x Red Hat Enterprise Linux for Power, little endian 10 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat Enterprise Linux for ARM 64 10 aarch64 - Extended Update Support 10.0 aarch64 Red Hat CodeReady Linux Builder for x86_64 10 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le Red Hat CodeReady Linux Builder for ARM 64 10 aarch64, IBM z Systems 10 s390x Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:15472 • https://access.redhat.com/errata/RHSA-2025:15447

Affected Product	**NetApp**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-56171, CVE-2025-27113, CVE-2024-42516, CVE-2024-53580, CVE-2025-24928, CVE-2023-39615)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause sensitive information disclosure, denial of service, addition or modification of data. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ONTAP 9 NetApp Manageability SDK NetApp HCI Compute Node (Bootstrap OS) Active IQ Unified Manager for VMware vSphere
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20250328-0010 • https://security.netapp.com/advisory/ntap-20250306-0004 • https://security.netapp.com/advisory/ntap-20250718-0013 • https://security.netapp.com/advisory/ntap-20250404-0009 • https://security.netapp.com/advisory/ntap-20250801-0009 • https://security.netapp.com/advisory/ntap-20250321-0006

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-6119, CVE-2024-47081, CVE-2025-50182, CVE-2025-50181, CVE-2024-12797)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar App SDK Versions - 1.0.0 - 2.2.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7244264

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-47561, CVE-2024-47554)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-47561 -** Schema parsing in the Java SDK of Apache Avro 1.11.3 and previous versions allows bad actors to execute arbitrary code. Users are recommended to upgrade to version 1.11.4 or 1.12.0, which fix this issue. **CVE-2024-47554 -** Uncontrolled Resource Consumption vulnerability in Apache Commons IO. The org.apache.commons.io.input.XmlStreamReader class may excessively consume CPU resources when processing maliciously crafted input. This issue affects Apache Commons IO: from 2.0 before 2.14.0. Users are recommended to upgrade to version 2.14.0 or later, which fixes the issue. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Intelligent Assurance - Prior to v4.2.7 - HPE Telco INT-A FAS and PDO
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04767en_us&docLocale=en_US

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-0395, CVE-2025-0690, CVE-2025-1125, CVE-2025-0689, CVE-2025-0686, CVE-2025-0624, CVE-2025-0622, CVE-2025-0677, CVE-2025-1118, CVE-2025-0725, CVE-2025-0167, CVE-2025-24928, CVE-2025-26465, CVE-2021-28041, CVE-2025-4517, CVE-2025-4330, CVE-2025-4138, CVE-2024-12718)
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 19.12 through 19.12.0.1 • NetWorker vProxy Versions prior to 19.11.0.6 • PowerScale OneFS Versions 9.5.0.0 through 9.10.1.2 • PowerScale OneFS Versions 9.7.0.0 through 9.7.1.9 • PowerScale OneFS Versions prior to 9.12.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000337955/dsa-2025-262-security-update-for-dell-networker-vproxy-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000363686/dsa-2025-319-security-update-for-dell-powerscale-onefs-multiple-vulnerabilities

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-42933, CVE-2025-42929, CVE-2025-42916, CVE-2025-27428, CVE-2025-22228, CVE-2025-42930, CVE-2025-42912, CVE-2025-42917, CVE-2023-5072, CVE-2025-42920, CVE-2025-42938, CVE-2025-42915, CVE-2025-42926, CVE-2025-42911, CVE-2025-42961, CVE-2025-42925, CVE-2025-42923, CVE-2025-42918, CVE-2025-42941, CVE-2025-42927, CVE-2024-13009)
Description	SAP has released monthly security updates addressing multiple vulnerabilities that exist in their Products. These vulnerabilities could be exploited by malicious users to cause directory traversal, security misconfiguration, denial of service, missing authorization check, cross-site scripting. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP Fiori (Launchpad) Version - SAP_UI 754 • SAP Business One (SLD) Version - B1_ON_HANA 10.0, SAP-M-BO 10.0 • SAP NetWeaver AS Java (Adobe Document Service) Version - ADSSAP 7.50 • SAP Commerce Cloud Version - HY_COM 2205, COM_CLOUD 2211 • SAP HCM (My Timesheet Fiori 2.0 application) Version - GBX01HR5 605 • SAP HCM (Approve Timesheets Fiori 2.0 application) Version - GBX01HR5 605 • SAP BusinessObjects Business Intelligence Platform Version - ENTERPRISE 430, 2025, 2027 • SAP Supplier Relationship Management Version – SRM_SERVER 700, 701, 702, 713, 714 • Fiori app (Manage Payment Blocks) Version - S4CORE 107, 108 • SAP NetWeaver Application Server Java Version - WD-RUNTIME 7.50 • SAP NetWeaver AS Java (IIOP Service) Version – SERVERCORE 7.50 • SAP Fiori App (F4044 Manage Work Center Groups) Version - UIS4HOP1 600, 700, 800, 900 • SAP S/4HANA (Private Cloud or On-Premise) Version - S4CORE 102, 103, 104, 105, 106, 107, 108 • SAP Landscape Transformation Replication Server Version - DMIS 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752, 2020 • SAP NetWeaver and ABAP Platform (Service Data Collection) Version - ST-PI 2008_1_700, 2008_1_710, 740 • SAP Commerce Cloud and SAP Datahub Version - HY_COM 2205, HY_DHUB 2205, COM_CLOUD 2211, DHUB_CLOUD 2211 • SAP Business Planning and Consolidation Version - BPC4HANA 200, 300, SAP_BW 750, 751, 752, 753, 754, 755, 756, 757, 758, 816, 914, CPMBPC 810 • SAP NetWeaver ABAP Platform Version - S4CRM 100, 200, 204, 205, 206, S4CEXT 109, BBPCRM 713, 714 • SAP NetWeaver (Service Data Download) Version - SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 816 • SAP NetWeaver Application Server for ABAP Version – SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 816 • SAP NetWeaver Application Server for ABAP (Background Processing) Version - SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 816
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/september-2025.html

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.