Advisory Alert

Alert Number: AAA20251014 **Date:** October 14, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SAP	**Critical**	Multiple Vulnerabilities
F5	**Critical**	Multiple Vulnerabilities
HPE	**High**	Arbitrary Code Execution Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Red Hat	**High**, Medium	Multiple Vulnerabilities
Ivanti	**High**, Medium	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
SAP	**High**, Medium, Low	Multiple Vulnerabilities
AMD	**Medium**	Improper Access Control Vulnerability

Description

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-42944, CVE-2025-42937, CVE-2025-42910)
Description	SAP has released monthly security updates addressing multiple vulnerabilities that exist in their Products. **CVE-2025-42944 -** Due to a deserialization vulnerability in SAP NetWeaver, an unauthenticated attacker could exploit the system through the RMI-P4 module by submitting malicious payload to an open port. The deserialization of such untrusted Java objects could lead to arbitrary OS command execution, posing a high impact to the application's confidentiality, integrity, and availability. **CVE-2025-42937 -** SAP Print Service (SAPSprint) performs insufficient validation of path information provided by users. An unauthenticated attacker could traverse to the parent directory and over-write system files causing high impact on confidentiality integrity and availability of the application. **CVE-2025-42910 -** Due to missing verification of file type or content, SAP Supplier Relationship Management allows an authenticated attacker to upload arbitrary files. These files could include executables which might be downloaded and executed by the user which could host malware. On successful exploitation an attacker could cause high impact on confidentiality, 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 AS Java Version - SERVERCORE 7.50 • SAP Print Service Versions - SAPSPRINT 8.00, 8.10 • SAP Supplier Relationship Management Versions - SRMNXP01 100, 150
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/october-2025.html

Affected Product	**F5**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-28863, CVE-2016-2148)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-28863 -** This vulnerability allows an attacker with network access to bypass the negotiated integrity and confidentiality in Intelligent Platform Management Interface (IPMI) v2.0 session parameters. This vulnerability affects Always-On Management (AOM) and platform security. **CVE-2016-2148 -** This vulnerability allows remote attackers to potentially perform a Remote Code Execution (RCE) using vectors involving OPTION_6RD parsing. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) Versions - 17.5.0 - 17.5.1, 17.1.0 - 17.1.3, 16.1.0 - 16.1.6, 15.1.0 - 15.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000156992 • https://my.f5.com/manage/s/article/K000156994

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2025-3052)
Description	HPE has released a security update addressing an arbitrary code execution vulnerability that exists in their products. This vulnerability could be locally exploited to allow security bypass. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Compute Scale-up Server 3200 - Prior to v1.65.60 HPE Superdome Flex 280 Server - Prior to v2.05.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04954en_us&docLocale=en_US

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-50154, CVE-2024-53168, CVE-2025-21692, CVE-2025-21791, CVE-2025-38477)
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	OpenSUSE Leap 15.3, 15.4 SUSE Linux Enterprise High Performance Computing 15 SP3, 15 SP4 SUSE Linux Enterprise Live Patching 15-SP3, 15-SP4 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP3, 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP3, 15 SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202503580-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503583-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503578-1/

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-53186, CVE-2023-53373, CVE-2025-38556, CVE-2025-38614, CVE-2025-39757, CVE-2025-39761, CVE-2022-50228, CVE-2023-53305)
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 Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux Server - AUS 9.2, 9.6 x86_64 Red Hat Enterprise Linux for x86_64 8, 9, 10 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6, 10.0 x86_64 Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64 Red Hat Enterprise Linux for Power, little endian 8, 9, 10 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6, 10.0 ppc64le Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for IBM z Systems 8, 9, 10 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6, 10.0 s390x Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6, 10.0 s390x Red Hat Enterprise Linux for ARM 64 8, 9, 10 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6, 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6, 9.2, 10.0 aarch64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64, 8 x86_64, 10 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6, 10.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8, 9, 10 ppc64le Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems 9, 10 s390x Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for ARM 64 8, 9, 10 aarch64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6, 10.0 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:17896 • https://access.redhat.com/errata/RHSA-2025:17760 • https://access.redhat.com/errata/RHSA-2025:17776 • https://access.redhat.com/errata/RHSA-2025:17797

Affected Product	**Ivanti**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-11622, CVE-2025-9713, CVE-2025-11623, CVE-2025-62392, CVE-2025-62390, CVE-2025-62389, CVE-2025-62388, CVE-2025-62387, CVE-2025-62385, CVE-2025-62391, CVE-2025-62383, CVE-2025-62386, CVE-2025-62384)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause privilege escalation, remote code execution, SQL injection, Path traversal. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Endpoint Manager Versions - 2022 SU8 SR2 and prior, 2024 SU3 SR1 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-EPM-October-2025?language=en_US

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20292, CVE-2025-43991)
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	Dell Connectrix MDS NX-OS Versions - prior to 9.4 (3a) Dell SupportAssist for Home PCs Versions - prior to 4.8.2.29006 Dell SupportAssist for Business PCs Versions - prior to 4.5.3.25254
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000379436/dsa-2025-378-security-update-for-dell-connectrix-mds-cisco-cli-vulnerability • https://www.dell.com/support/kbdoc/en-us/000378367/dsa-2025-362-security-update-for-dell-supportassist-for-home-pcs-and-dell-supportassist-for-business-pcs-vulnerabilities

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-5115, CVE-2025-48913, CVE-2025-0059, CVE-2025-42901, CVE-2025-42908, CVE-2025-42906, CVE-2025-42902, CVE-2025-42939, CVE-2025-31331, CVE-2025-42903, CVE-2025-31672, CVE-2025-42909)
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 information disclosure, denial of service, code injection, cross-site request forgery, directory traversal and authorization bypass. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP Commerce Cloud Versions - HY_COM 2205, COM_CLOUD 2211, 2211-JDK21 • SAP Data Hub Integration Suite Version - CX_DATAHUB_INT_PACK 2205 • SAP NetWeaver Application Server ABAP Versions – KRNL64UC 7.53, KERNEL 7.53, 7.54, 7.77, 7.89, 7.93, 9.12, 9.14 • SAP Application Server for ABAP Versions - SAP_BASIS 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 758, 816 • SAP NetWeaver Application Server for ABAP Versions - KRNL64UC 7.53, KERNEL 7.53, 7.54, 7.77, 7.89, 7.93, 9.16 • SAP Commerce Cloud Version - COM_CLOUD 2211 • SAP NetWeaver AS ABAP and ABAP Platform Versions - KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 9.14, 9.15, 9.16 • SAP S/4HANA Versions - S4CORE 104, 105, 106, 107, 108, 109 • SAP NetWeaver Versions - SAP_ABA 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, 75I • SAP Financial Service Claims Management Versions - INSURANCE 803, 804, 805, 806, S4CEXT 107, 108, 109 • SAP BusinessObjects Versions - ENTERPRISE 430, 2025, 2027 • SAP Cloud Appliance Library Appliances Version - TITANIUM_WEBAPP 4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/october-2025.html

Affected Product	**AMD**
Severity	**Medium**
Affected Vulnerability	Improper Access Control Vulnerability (CVE-2025-0033)
Description	AMD has released security updates addressing an improper access control vulnerability that exist in their products. **CVE-2025-0033 -** Improper access control within AMD SEV-SNP could allow an admin-privileged attacker to write to the RMP during SNP initialization, potentially resulting in a loss of SEV-SNP guest memory integrity. AMD advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	AMD EPYC 7003 Series Processors - Milan, Milan-X AMD EPYC 8004 Series Processors AMD EPYC 9004 Series Processors - Siena, Genoa, Genoa-X, Bergamo AMD EPYC 9005 Series Processors - Turin AMD EPYC Embedded 8004 Series Processors - Embedded Siena AMD EPYC Embedded 9004 Series Processors - Embedded Genoa AMD EPYC Embedded 9004 Series Processors - Embedded Bergamo
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-3020.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.