Advisory Alert

Alert Number: **AAA20251112** **Date:** **November 12, 2025**

Document Classification Level **:** Public Circulation Permitted | Public

Information Classification Level **:** TLP: WHITE

Overview

Product	Severity	Vulnerability
SAP	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
Lenovo	**High**	Multiple Vulnerabilities
Ivanti	**High**	Security Update
SUSE	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
Dell	**High, Medium**	Multiple Vulnerabilities
Intel	**High, Medium, Low**	Multiple Vulnerabilities
SAP	**High, Medium, Low**	Multiple Vulnerabilities
Citrix	**Medium**	Cross-Site Scripting Vulnerability

Description

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-42887, CVE-2025-42944, CVE-2025-42890)
Description	SAP has released monthly security updates addressing multiple vulnerabilities that exist in their Products. **CVE-2025-42887 -** Due to missing input sanitation, SAP Solution Manager allows an authenticated attacker to insert malicious code when calling a remote-enabled function module. This could provide the attacker with full control of the system hence leading to high impact on confidentiality, integrity and availability of the system. **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-2025-42890 -** SQL Anywhere Monitor (Non-GUI) baked credentials into the code,exposing the resources or functionality to unintended users and providing attackers with the possibility of arbitrary code execution.This could cause high impact on confidentiality integrity and availability of the system. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SAP Solution Manager Versions - ST 720 SAP NetWeaver AS Java Versions - SERVERCORE 7.50 SQL Anywhere Monitor (Non-Gui) Versions -SYBASE_SQL_ANYWHERE_SERVER 17.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/november-2025.html

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-9132, CVE-2025-10585, CVE-2025-10500, CVE-2025-10501, CVE-2025-10502, CVE-2025-11205, CVE-2025-11206, CVE-2025-11207, CVE-2025-11208, CVE-2025-11209, CVE-2025-11210, CVE-2025-11211, CVE-2025-11212, CVE-2025-11213, CVE-2025-11215, CVE-2025-11216, CVE-2025-11219)
Description	Dell 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. 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/000379460/dsa-2025-389-security-update-for-dell-thinos-10-for-multiple-google-chrome-vulnerabilities

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-62203, CVE-2025-60727, CVE-2025-60726, CVE-2025-62222, CVE-2025-62213, CVE-2025-62209, CVE-2025-62208, CVE-2025-60724, CVE-2025-60717, CVE-2025-60716, CVE-2025-60713, CVE-2025-59515, CVE-2025-62452, CVE-2025-62220, CVE-2025-62219, CVE-2025-60719, CVE-2025-60708, CVE-2025-60704, CVE-2025-59512, CVE-2025-59508, CVE-2025-30398, CVE-2025-62453, CVE-2025-60721, CVE-2025-62449, CVE-2025-62215, CVE-2025-62214, CVE-2025-62211, CVE-2025-59499, CVE-2025-62205, CVE-2025-62204, CVE-2025-62202, CVE-2025-62201, CVE-2025-62200, CVE-2025-60723, CVE-2025-60720, CVE-2025-60718, CVE-2025-60715, CVE-2025-60714, CVE-2025-59514, CVE-2025-47179, CVE-2025-59240, CVE-2025-62218, CVE-2025-62217, CVE-2025-60722, CVE-2025-62216, CVE-2025-62210, CVE-2025-62206, CVE-2025-62199, CVE-2025-60728, CVE-2025-60710, CVE-2025-60709, CVE-2025-60707, CVE-2025-60706, CVE-2025-60705, CVE-2025-60703, CVE-2025-59513, CVE-2025-59511, CVE-2025-59510, CVE-2025-59509, CVE-2025-59507, CVE-2025-59506, CVE-2025-59505, CVE-2025-59504, CVE-2025-62230, CVE-2025-61104, CVE-2025-61100, CVE-2025-61101, CVE-2025-40106, CVE-2025-12060)
Description	Microsoft has released monthly security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause remote code execution, information disclosure, elevation of privilege, denial of service. security feature bypass and spoofing. Microsoft advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	azl3 frr 9.1.1-3 azl3 keras 3.3.3-4 azl3 kernel 6.6.104.2-4 azl3 xorg-x11-server-Xwayland 24.1.6-2 Azure Monitor cbl2 frr 8.5.5-3 Dynamics 365 Field Service (online) Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft Configuration Manager 2403 Microsoft Configuration Manager 2409 Microsoft Configuration Manager 2503 Microsoft Dynamics 365 (on-premises) version 9.1 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 SharePoint Enterprise Server 2016 Microsoft SharePoint Server 2019 Microsoft SharePoint Server Subscription Edition Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR) Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 Azure Connect Feature Pack Microsoft SQL Server 2017 for x64-based Systems (CU 31) Microsoft SQL Server 2017 for x64-based Systems (GDR) Microsoft SQL Server 2019 for x64-based Systems (CU 32) Microsoft SQL Server 2019 for x64-based Systems (GDR) Microsoft SQL Server 2022 for x64-based Systems (CU 21) Microsoft SQL Server 2022 for x64-based Systems (GDR) Microsoft Visual Studio 2022 version 17.14 Microsoft Visual Studio Code CoPilot Chat Extension Nuance PowerScribe 360 version 4.0.1 Nuance PowerScribe 360 version 4.0.2 Nuance PowerScribe 360 version 4.0.3 Nuance PowerScribe 360 version 4.0.4 Nuance PowerScribe 360 version 4.0.5 Nuance PowerScribe 360 version 4.0.6 Nuance PowerScribe 360 version 4.0.7 Nuance PowerScribe 360 version 4.0.8 Nuance PowerScribe 360 version 4.0.9 Nuance PowerScribe One version 2019.1 Nuance PowerScribe One version 2019.10 Nuance PowerScribe One version 2019.2 Office Online Server OneDrive for Android PowerScribe One version 2023.1 SP2 Patch 7 Visual Studio Code 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 11 Version 25H2 for ARM64-based Systems Windows 11 Version 25H2 for x64-based Systems 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 Windows Server 2012 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation) Windows Server 2016 Windows Server 2016 (Server Core installation) Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server 2022 Windows Server 2022 (Server Core installation) Windows Server 2022, 23H2 Edition (Server Core installation) Windows Server 2025 Windows Server 2025 (Server Core installation) Windows Subsystem for Linux GUI Nuance PowerScribe One version 2019.3 Nuance PowerScribe One version 2019.4 Nuance PowerScribe One version 2019.5 Nuance PowerScribe One version 2019.6 Nuance PowerScribe One version 2019.7 Nuance PowerScribe One version 2019.8 Nuance PowerScribe One version 2019.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/vulnerability

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38805, CVE-2025-29934, CVE-2025-30185, CVE-2025-35968)
Description	Lenovo 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 and privilege escalation. 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-207908

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2025-10918)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-10918 -** Insecure default permissions in the agent of Ivanti Endpoint Manager before version 2024 SU4 allows a local authenticated attacker to write arbitrary files anywhere on disk. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Endpoint Manager Versions - Prior to 2024 SU3 SR1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-EPM-November-2025-for-EPM-2024?language=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	Basesystem Module 15-SP7 Development Tools Module 15-SP7 Legacy Module 15-SP7 OpenSUSE Leap 15.4, 15.5 SUSE Linux Enterprise Desktop 15 SP7 SUSE Linux Enterprise High Availability Extension 15 SP7 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP4, 15-SP5, 15-SP7 SUSE Linux Enterprise Micro 5.3, 5.4, 5.5 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5, 15 SP7 SUSE Linux Enterprise Server 12 SP5, 15 SP4, 15 SP5, 15 SP7 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP4, 15 SP5, 15 SP7 SUSE Linux Enterprise Workstation Extension 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20254046-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254043-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254050-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20252264-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20252173-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254056-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254057-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254058-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254059-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254062-1/

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-30185, CVE-2025-29934)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-30185 -** Potential security vulnerabilities in HPE ProLiant DL, and Synergy servers using certain Intel processors could be locally exploited to allow escalation of privilege, and denial of service. For more information on these vulnerabilities, please see Intel Security Advisory INTEL-SA-01378, UPLR1 - Intel UEFI Server Firmware Advisory. **CVE-2025-29934 -** A potential security vulnerability in HPE ProLiant DL/XL servers using AMD EPYC processors could be locally exploited to allow unauthorized access. For more information on the vulnerability, please see AMD Security Bulletin, AMD-SB-3029: Stale Translation Lookaside Buffer (TLB) Entry Vulnerability. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE ProLiant Compute DL320 Gen12 - Prior to 1.50_09-05-2025 HPE ProLiant Compute DL325 Gen12 - Prior to 1.10_05-27-2025 HPE ProLiant Compute DL340 Gen12 - Prior to 1.50_09-05-2025 HPE ProLiant Compute DL345 Gen12 - Prior to 1.10_05-27-2025 HPE ProLiant Compute DL360 Gen12 - Prior to 1.50_09-05-2025 HPE ProLiant Compute DL380 Gen12 - Prior to 1.50_09-05-2025 HPE ProLiant Compute DL380a Gen12 - Prior to 1.50_09-05-2025 HPE ProLiant Compute DL580 Gen12 - Prior to 1.50_09-05-2025 HPE ProLiant Compute ML350 Gen12 - Prior to 1.50_09-05-2025 HPE ProLiant Compute XD230 - Prior to 1.50_09-05-2025 HPE ProLiant DL145 Gen11 - Prior to 1.70_08-07-2025 HPE ProLiant DL325 Gen10 Plus server - Prior to 3.60_01-16-2025 HPE ProLiant DL325 Gen10 Plus v2 server - Prior to 3.60_01-16-2025 HPE ProLiant DL325 Gen11 Server - Prior to 2.70_08-07-2025 HPE ProLiant DL345 Gen10 Plus server - Prior to 3.60_01-16-2025 HPE ProLiant DL345 Gen11 Server - Prior to 2.70_08-07-2025 HPE ProLiant DL365 Gen10 Plus server - Prior to 3.60_01-16-2025 HPE ProLiant DL365 Gen11 Server - Prior to 2.70_08-07-2025 HPE ProLiant DL385 Gen10 Plus server - Prior to 3.60_01-16-2025 HPE ProLiant DL385 Gen10 Plus v2 server - Prior to 3.60_01-16-2025 HPE ProLiant DL385 Gen11 Server - Prior to 2.70_08-07-2025 HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to 3.60_01-16-2025 HPE Synergy 480 Gen12 Compute Module - Prior to 1.50_09-05-2025
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04962en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04965en_us&docLocale=en_US

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000373430/dsa-2025-367-security-update-for-dell-client-platform-for-intel-proset-wireless-wi-fi-software-advisory • https://www.dell.com/support/kbdoc/en-us/000376224/dsa-2025-333-security-update-for-dell-powerprotect-data-domain-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000326043/dsa-2025-227 • https://www.dell.com/support/kbdoc/en-us/000359232/dsa-2025-328

Affected Product	**Intel**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/default.html

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-42940, CVE-2025-42895, CVE-2025-42892, CVE-2025-42894, CVE-2025-42884, CVE-2025-42924, CVE-2025-42893, CVE-2025-42886, CVE-2025-42885, CVE-2025-42888, CVE-2025-42889, CVE-2025-42919, CVE-2025-42897, CVE-2025-42899, CVE-2025-42882, CVE-2025-23191, CVE-2025-42883)
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 Memory Corruption, Code Injection, Path Traversal and Information Disclosure. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP CommonCryptoLib Version(s) - CRYPTOLIB 8 • SAP HANA JDBC Client Version(s) - HDB_CLIENT 2.0 • SAP Business Connector Version(s) - SAP BC 4.8 • SAP Business Connector Version(s) - SAP BC 4.8 • SAP NetWeaver Enterprise Portal Version(s) - EP-BASIS 7.50, EP-RUNTIME 7.50 • SAP S/4HANA landscape (SAP E-Recruiting BSP) Version(s) - S4ERECRT 100, 200, ERECRUIT 600, 603, 604, 605, 606, 616, 617, 800, 801, 802 • SAP Business Connector Version(s) - SAP BC 4.8 • SAP Business Connector Version(s) - SAP BC 4.8 • SAP HANA 2.0 (hdbrss) Version(s) - HDB 2.00 • SAP GUI for Windows Version(s) - BC-FES-GUI 8.00, 8.10 • SAP Starter Solution (PL SAFT) Version(s) - SAP_APPL 600, 602, 603, 604, 605, 606, 616, SAP_FIN 617, 618, 700, 720, 730, S4CORE 100, 101, 102, 103, 104 • SAP NetWeaver Application Server Java Version(s) - ENGINEAPI 7.50, EP-BASIS 7.50 • SAP Business One (SLD) Version(s) - B1_ON_HANA 10.0, SAP-M-BO 10.0 • SAP S4CORE (Manage Journal Entries) Version(s) - S4CORE 104, 105, 106, 107, 108 • SAP NetWeaver Application Server for ABAP Version(s) - 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 Fiori for SAP ERP Version(s) – SAP_GWFND 740, 750, 751, 752, 753, 754, 755, 756, 757, 758 • SAP NetWeaver Application Server for ABAP (Migration Workbench) Version(s) - 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/november-2025.html

Affected Product	**Citrix**
Severity	**Medium**
Affected Vulnerability	Cross-Site Scripting Vulnerability (CVE-2025-12101)
Description	Citrix has released security updates addressing a cross-site scripting vulnerability that exists in their products. This vulnerabilities could be exploited by malicious users to compromise affected systems. Citrix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-56.73 NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-60.32 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.250-FIPS and NDcPP NetScaler ADC 12.1-FIPS and NDcPP BEFORE 12.1-55.333-FIPS and NDcPP
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX695486&articleURL=NetScaler_ADC_and_NetScaler_Gateway_Security_Bulletin_for_CVE_2025_12101

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.