Advisory Alert

Alert Number: AAA20250813 **Date:** August 13, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SAP	**Critical**	Multiple Vulnerabilities
Fortinet	**Critical**	Remote Unauthenticated Command Injection Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Fortinet	**High**, Medium	Multiple Vulnerabilities
Intel	**High**, Medium, Low	Multiple Vulnerabilities
SAP	**High**, Medium, Low	Multiple Vulnerabilities
Palo Alto	Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-42957, CVE-2025-42950, CVE-2025-27429)
Description	SAP has released monthly security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-42957, CVE-2025-27429** - SAP S/4HANA allows an attacker with user privileges to exploit a vulnerability in the function module exposed via RFC. This flaw enables the injection of arbitrary ABAP code into the system, bypassing essential authorization checks. This vulnerability effectively functions as a backdoor, creating the risk of full system compromise, undermining the confidentiality, integrity and availability of the system. **CVE-2025-42950** - SAP Landscape Transformation (SLT) allows an attacker with user privileges to exploit a vulnerability in the function module exposed via RFC. This flaw enables the injection of arbitrary ABAP code into the system, bypassing essential authorization checks. This vulnerability effectively functions as a backdoor, creating the SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP S/4HANA (Private Cloud or On-Premise) Version - S4CORE 102, 103, 104, 105, 106, 107, 108 • SAP Landscape Transformation (Analysis Platform) Version - DMIS 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752, 2020
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/august-2025.html

Affected Product	**Fortinet**
Severity	**Critical**
Affected Vulnerability	Remote Unauthenticated Command Injection Vulnerability (CVE-2025-25256)
Description	Fortinet has released security updates addressing a remote unauthenticated command injection vulnerability that exists in their products. **CVE-2025-25256** - An improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in FortiSIEM may allow an unauthenticated attacker to execute unauthorized code or commands via crafted CLI requests. Fortinet advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiSIEM 6.6 - 6.6 all versions FortiSIEM 6.5 - 6.5 all versions FortiSIEM 6.4 - 6.4 all versions FortiSIEM 6.3 - 6.3 all versions FortiSIEM 6.2 - 6.2 all versions FortiSIEM 6.1 - 6.1 all versions FortiSIEM 5.4 - 5.4 all versions FortiSIEM 7.3 - 7.3.0 through 7.3.1 FortiSIEM 7.2 - 7.2.0 through 7.2.5 FortiSIEM 7.1 - 7.1.0 through 7.1.7 FortiSIEM 7.0 - 7.0.0 through 7.0.3 FortiSIEM 6.7 - 6.7.0 through 6.7.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-25-152

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-53724, CVE-2025-48807, CVE-2025-53789, CVE-2025-53784, CVE-2025-53783, CVE-2025-53778, CVE-2025-50155, CVE-2025-53766, CVE-2025-53737, CVE-2025-53736, CVE-2025-53735, CVE-2025-53733, CVE-2025-53732, CVE-2025-53731, CVE-2025-47954, CVE-2025-53728, CVE-2025-53726, CVE-2025-53725, CVE-2025-53779, CVE-2025-53765, CVE-2025-53740, CVE-2025-53739, CVE-2025-53738, CVE-2025-53718, CVE-2025-53716, CVE-2025-49736, CVE-2025-49712, CVE-2025-49707, CVE-2025-49755, CVE-2025-53734, CVE-2025-53723, CVE-2025-53722, CVE-2025-53721, CVE-2025-53153, CVE-2025-53148, CVE-2025-53144, CVE-2025-53141, CVE-2025-53140, CVE-2025-53136, CVE-2025-53133, CVE-2025-53132, CVE-2025-50176, CVE-2025-53793, CVE-2025-50157, CVE-2025-53152, CVE-2025-53147, CVE-2025-50173, CVE-2025-50168, CVE-2025-50167, CVE-2025-50163, CVE-2025-50162, CVE-2025-50159, CVE-2025-50154, CVE-2025-50153, CVE-2025-53781, CVE-2025-53773, CVE-2025-53772, CVE-2025-24999, CVE-2025-53788, CVE-2025-53769, CVE-2025-53720, CVE-2025-53719, CVE-2025-53156, CVE-2025-53155, CVE-2025-53154, CVE-2025-53151, CVE-2025-53149, CVE-2025-53145, CVE-2025-53143, CVE-2025-53142, CVE-2025-53138, CVE-2025-53137, CVE-2025-53135, CVE-2025-53134, CVE-2025-53131, CVE-2025-50177, CVE-2025-50172, CVE-2025-50171, CVE-2025-50170, CVE-2025-50169, CVE-2025-50166, CVE-2025-50165, CVE-2025-50164, CVE-2025-50161, CVE-2025-50160, CVE-2025-50158, CVE-2025-50156, CVE-2025-49762, CVE-2025-49761, CVE-2025-49759, CVE-2025-49757, CVE-2025-49743, CVE-2025-25007, CVE-2025-25006, CVE-2025-25005, CVE-2025-53761, CVE-2025-53760, CVE-2025-53759, CVE-2025-53741, CVE-2025-53730, CVE-2025-33051, CVE-2025-53729, CVE-2025-53727, CVE-2025-49758, CVE-2025-49745, CVE-2025-49751, CVE-2025-53786, CVE-2025-8583, CVE-2025-8582, CVE-2025-8581, CVE-2025-8580, CVE-2025-8579, CVE-2025-8578, CVE-2025-8577, CVE-2025-8576, CVE-2025-53787, CVE-2025-53774, CVE-2025-53767, CVE-2025-53792, CVE-2025-8292)
Description	Microsoft 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. Microsoft advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Teams Panels Teams Phones Web Deploy 4.0 Azure File Sync v18 Azure File Sync v19 Azure File Sync v20 Azure File Sync v21 Azure Open AI Azure Portal Azure Stack Hub Azure Stack Hub 2406 Azure Stack Hub 2408 Azure Stack Hub 2501 DCadsv5-series Azure VM DCasv5-series Azure VM DCedsv5-series Azure VM DCesv5-series - Azure VM DCesv6-series Azure VM ECadsv5-series Azure VM ECasv5-series Azure VM ECedsv5-series Azure VM ECesv5-series Azure VM Ecesv6-series Azure VM NCCadsH100v5-series Azure VM Office Online Server Microsoft Teams for Android Microsoft Teams for Desktop Microsoft Teams for iOS Microsoft Teams for Mac Teams for D365 Guides Hololens Teams for D365 Remote Assist HoloLens Microsoft Word 2016 (32-bit edition) Microsoft Word 2016 (64-bit edition) Windows 10 for 32-bit Systems Windows 10 for x64-based Systems Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft 365 Copilot's Business Chat Microsoft Dynamics 365 (on-premises) version 9.1 Microsoft Edge (Chromium-based) Microsoft Edge for Android 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 for Universal Microsoft Office LTSC for Mac 2021 Microsoft Office LTSC for Mac 2024 Microsoft PowerPoint 2016 (32-bit edition) Microsoft PowerPoint 2016 (64-bit edition) Microsoft SharePoint Enterprise Server 2016 Microsoft SharePoint Server 2019	Microsoft Exchange Server 2016 Cumulative Update 23 Microsoft Exchange Server 2019 Cumulative Update 14 Microsoft Exchange Server 2019 Cumulative Update 15 Microsoft Exchange Server Subscription Edition RTM 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), (GDR) Microsoft SQL Server 2019 for x64-based Systems (CU 32), (GDR) Microsoft SQL Server 2022 for x64-based Systems (CU 20), (GDR) 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 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 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) Microsoft Visual Studio 2022 version 17.14 Windows Server 2025 Windows Server 2025 (Server Core installation) Windows Subsystem for Linux (WSL2) 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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/vulnerability

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-49788, CVE-2022-50020, CVE-2022-50022, CVE-2024-57980, CVE-2024-58002, CVE-2025-21727, CVE-2025-21919, CVE-2025-21928, CVE-2025-23150, CVE-2025-38052, CVE-2025-38086, CVE-2025-38380)
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 8.6 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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:13776

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-36348, CVE-2024-36349, CVE-2024-36350, CVE-2024-36357, CVE-2024-45332, CVE-2025-20629, CVE-2023-20599, CVE-2024-39286, CVE-2025-26403, CVE-2025-32086)
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 PowerEdge R770 BIOS - Versions prior to 1.3.2 Dell PowerEdge R670 BIOS - Versions prior to 1.3.2 Dell PowerEdge R570 BIOS - Versions prior to 1.3.2 Dell PowerEdge R470 BIOS - Versions prior to 1.3.2 Dell PowerEdge XE7740 BIOS - Versions prior to 1.2.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000356015/dsa-2025-323-dell-poweredge-server-security-update-for-intel-xeon-6-processor-firmware-vulnerabilities

Affected Product	**Fortinet**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-32932, CVE-2024-26009, CVE-2025-32766, CVE-2024-40588, CVE-2024-48892, CVE-2025-49813, CVE-2025-25248, CVE-2025-53744, CVE-2023-45584, CVE-2025-47857, CVE-2025-27759, CVE-2025-52970, CVE-2024-52964)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to Improper access control, Information disclosure, denial of service, privilege escalation. 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-24-513 • https://www.fortiguard.com/psirt/FG-IR-24-042 • https://www.fortiguard.com/psirt/FG-IR-25-383 • https://www.fortiguard.com/psirt/FG-IR-24-309 • https://www.fortiguard.com/psirt/FG-IR-24-421 • https://www.fortiguard.com/psirt/FG-IR-24-421 • https://www.fortiguard.com/psirt/FG-IR-25-501 • https://www.fortiguard.com/psirt/FG-IR-24-364 • https://www.fortiguard.com/psirt/FG-IR-25-173 • https://www.fortiguard.com/psirt/FG-IR-23-209 • https://www.fortiguard.com/psirt/FG-IR-25-253 • https://www.fortiguard.com/psirt/FG-IR-25-150 • https://www.fortiguard.com/psirt/FG-IR-25-448 • https://www.fortiguard.com/psirt/FG-IR-24-473

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 cause Privilege Escalation, Denial of Service, and Information Disclosure. 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-2025-42951, CVE-2025-42976, CVE-2025-42946, CVE-2025-42945, CVE-2025-42942, CVE-2025-42948, CVE-2025-0059, CVE-2025-42936, CVE-2025-23194, CVE-2025-42949, CVE-2025-42943, CVE-2025-42934, CVE-2025-31331, CVE-2025-42935, CVE-2025-42955, CVE-2025-42941)
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 Improper access Control, Privilege escalation, Out-of-bounds Read/write, information discloser. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP Business One (SLD) Version - B1_ON_HANA 10.0, SAP-M-BO 10.0 • SAP NetWeaver Application Server ABAP (BIC Document) Version - S4COREOP 104, 105, 106, 107, 108, SEM-BW 600, 602, 603, 604, 605, 634, 736, 746, 747, 748 • SAP S/4HANA (Bank Communication Management) Version - SAP_APPL 606, SAP_FIN 617, 618, 720, 730, S4CORE 102, 103, 104, 105, 106, 107, 108 • SAP NetWeaver Application Server ABAP Version - KRNL64UC 7.53, KERNEL 7.53, 7.54, 7.77, 7.89, 7.93 • 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_BASIS 914, SAP_BASIS 916 • SAP NetWeaver ABAP Platform Version - S4CRM 100, 200, 204, 205, 206, S4CEXT 107, 108, 109, BBPCRM 713, 714 • SAP NetWeaver Application Server ABAP (applications based on SAP GUI for HTML) Version – KRNL64UC 7.53, KERNEL 7.53, 7.54, 7.77, 7.89, 7.93, 9.12, 9.14 • SAP NetWeaver Enterprise Portal (OBN component) Version – EP-RUNTIME 7.50 • SAP GUI for Windows Version - BC-FES-GUI 8.00 • SAP S/4HANA (Supplier invoice) Version - S4CORE 102, 103, 104, 105, 106, 107, 108, 109 • SAP NetWeaver Version – SAP_ABA 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, 75I • SAP NetWeaver AS for ABAP and ABAP Platform(Internet Communication Manager) Version - 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 Cloud Connector Version - SAP_CLOUD_CONNECTOR 2.0 • SAP Fiori (Launchpad) Version - SAP_UI 754 • ABAP Platform Version - SAP_BASIS 758, SAP_BASIS 816, SAP_BASIS 916
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/august-2025.html

Affected Product	**Palo Alto**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-0141, CVE-2025-0135)
Description	Palo Alto has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-0141** - An incorrect privilege assignment vulnerability in the Palo Alto Networks GlobalProtect App on enables a locally authenticated non administrative user to escalate their privileges to root on macOS and Linux or NT AUTHORITY\SYSTEM on Windows. **CVE-2025-0135** - An incorrect privilege assignment vulnerability in the Palo Alto Networks GlobalProtect app on macOS devices enables a locally authenticated non administrative user to disable the app even if the GlobalProtect app configuration would not normally permit them to do so. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	GlobalProtect App 6.3 Versions - prior to 6.3.3-h1 (6.3.3-c650), 6.3.3-h2 (6.3.3-c676) on macOS GlobalProtect App 6.3 Versions - prior to 6.3.3-h1 (6.3.3-c650) on Windows GlobalProtect App 6.2 Versions - prior to 6.2.8-h2 (6.2.8-c243), 6.2.8-h3 (6.2.8-c263) on macOS GlobalProtect App 6.2 Versions - prior to 6.2.8-h2 (6.2.8-c243) on Windows GlobalProtect App 6.2 Versions - prior to 6.2.8 on Linux GlobalProtect App 6.1, 6.0 All on macOS, Windows, Linux
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.paloaltonetworks.com/CVE-2025-0141 • https://security.paloaltonetworks.com/CVE-2025-0135

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.