Advisory Alert

Alert Number: AAA20250409 **Date:** April 9, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
FortiGuard	**Critical**	Unverified Password Change Vulnerability
SAP	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
Ivanti	**High**, Medium	Multiple Vulnerabilities
FortiGuard	**High**, Medium, Low	Multiple Vulnerabilities
SAP	**High**, Medium, Low	Multiple Vulnerabilities
F5	Low	Security Update

Description

Affected Product	**FortiGuard**
Severity	**Critical**
Affected Vulnerability	Unverified Password Change Vulnerability (CVE-2024-48887)
Description	FortiGuard has released security updates addressing an Unverified Password Change Vulnerability that exists in FortiSwitch GUI. This vulnerability allows a remote unauthenticated attacker to modify admin passwords via a specially crafted request. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiSwitch 7.6 version 7.6.0 FortiSwitch 7.4 versions 7.4.0 through 7.4.4 FortiSwitch 7.2 versions 7.2.0 through 7.2.8 FortiSwitch 7.0 versions 7.0.0 through 7.0.10 FortiSwitch 6.4 versions 6.4.0 through 6.4.14
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-24-435

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-27429, CVE-2025-31330, CVE-2025-30016)
Description	SAP has released monthly security updates addressing multiple vulnerabilities that exist in their products. **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-2025-31330** - 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 risk of full system compromise, undermining the confidentiality, integrity and availability of the system. **CVE-2025-30016** - SAP Financial Consolidation allows an unauthenticated attacker to gain unauthorized access to the Admin account. The vulnerability arises due to improper authentication mechanisms, due to which there is high impact on the Confidentiality, Integrity & Availability of the application. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP S/4HANA (Private Cloud), Versions - S4CORE 102, 103, 104, 105, 106, 107, 108 • SAP Landscape Transformation (Analysis Platform), Versions - DMIS 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731 • SAP Financial Consolidation, Version - FINANCE 1010
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-27736, CVE-2025-27735, CVE-2025-27732, CVE-2025-27492, CVE-2025-27487, CVE-2025-27481, CVE-2025-27480, CVE-2025-27484, CVE-2025-29811, CVE-2025-29809, CVE-2025-29802, CVE-2025-29800, CVE-2025-29803, CVE-2025-27739, CVE-2025-26682, CVE-2025-24062, CVE-2025-24060, CVE-2025-27491, CVE-2025-20570, CVE-2025-27483, CVE-2025-27482, CVE-2025-27490, CVE-2025-29804, CVE-2025-29801, CVE-2025-27730, CVE-2025-27727, CVE-2025-27485, CVE-2025-27467, CVE-2025-26675, CVE-2025-27738, CVE-2025-29819, CVE-2025-29816, CVE-2025-27737, CVE-2025-27731, CVE-2025-26679, CVE-2025-29812, CVE-2025-29810, CVE-2025-26671, CVE-2025-26648, CVE-2025-24073, CVE-2025-27741, CVE-2025-27477, CVE-2025-27473, CVE-2025-26687, CVE-2025-26668, CVE-2025-26666, CVE-2025-27728, CVE-2025-27469, CVE-2025-26673, CVE-2025-26640, CVE-2025-26642, CVE-2025-21221, CVE-2025-21205, CVE-2025-27749, CVE-2025-26665, CVE-2025-29805, CVE-2025-29808, CVE-2025-27733, CVE-2025-27729, CVE-2025-27486, CVE-2025-27489, CVE-2025-26678, CVE-2025-26676, CVE-2025-26672, CVE-2025-26674, CVE-2025-26670, CVE-2025-26652, CVE-2025-26651, CVE-2025-26647, CVE-2025-26649, CVE-2025-26644, CVE-2025-26641, CVE-2025-26637, CVE-2025-26635, CVE-2025-26639, CVE-2025-26628, CVE-2025-25002, CVE-2025-24058, CVE-2025-21222, CVE-2025-21204, CVE-2025-21203, CVE-2025-21191, CVE-2025-21197, CVE-2025-21174, CVE-2025-24074, CVE-2025-29824, CVE-2025-29823, CVE-2025-29822, CVE-2025-29820, CVE-2025-29821, CVE-2025-29794, CVE-2025-29792, CVE-2025-29793, CVE-2025-29791, CVE-2025-27750, CVE-2025-27752, CVE-2025-27751, CVE-2025-27743, CVE-2025-27747, CVE-2025-27748, CVE-2025-27746, CVE-2025-27745, CVE-2025-27742, CVE-2025-27744, CVE-2025-27740, CVE-2025-27479, CVE-2025-27478, CVE-2025-27475, CVE-2025-27476, CVE-2025-27474, CVE-2025-27472, CVE-2025-27470, CVE-2025-27471, CVE-2025-26688, CVE-2025-26686, CVE-2025-26680, CVE-2025-26681, CVE-2025-26667, CVE-2025-26669, CVE-2025-26664, CVE-2025-26663)
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	Windows 11 Version 23H2 for ARM64-based Systems Windows Server 2025 (Server Core installation) Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 for x64-based Systems Windows 10 for 32-bit Systems Windows Server 2025 Windows 10 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2016 (Server Core installation) Windows Server 2016 Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows Server 2022 (Server Core installation) Windows Server 2022 Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 10 Version 21H2 for x64-based Systems Microsoft Visual Studio 2022 version 17.10 Microsoft Visual Studio 2022 version 17.8 Microsoft AutoUpdate for Mac SQL Server Management Studio 20.2 VSTA 2019 SDK VSTA 2022 SDK Visual Studio Tools for Applications (VSTA) 2022 Visual Studio Tools for Applications (VSTA) 2019 Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Microsoft Visual Studio 2022 version 17.13 Microsoft Visual Studio 2022 version 17.12 ASP.NET Core 8.0 Visual Studio Code ASP.NET Core 9.0 Windows Admin Center Windows Admin Center in Azure Portal Microsoft Word 2016 (64-bit edition) Microsoft Word 2016 (32-bit edition) Microsoft Office 2016 (64-bit edition) Microsoft Office 2016 (32-bit edition) Microsoft Office LTSC for Mac 2024 Microsoft Office LTSC 2024 for 64-bit editions Microsoft Office LTSC 2024 for 32-bit editions Microsoft Office LTSC 2021 for 32-bit editions Microsoft Office LTSC 2021 for 64-bit editions Microsoft Office LTSC for Mac 2021 Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft Office 2019 for 64-bit editions Microsoft Office 2019 for 32-bit editions Remote Desktop client for Windows Desktop Windows App Client for Windows Desktop Microsoft Access 2016 (64-bit edition) Microsoft Outlook for Android Azure Stack HCI OS 23H2 Azure Stack HCI OS 22H2 Microsoft Access 2016 (32-bit edition) Microsoft Excel 2016 (64-bit edition) Microsoft Excel 2016 (32-bit edition) Microsoft SharePoint Server 2019 Office Online Server Azure Local Cluster Microsoft OneNote 2016 (64-bit edition) Microsoft OneNote 2016 (32-bit edition) Microsoft OneNote for Mac Microsoft SharePoint Enterprise Server 2016 Microsoft Dynamics 365 Business Central 2025 Wave 1 – Update 26.0 Microsoft Dynamics 365 Business Central 2024 Wave 2 – Update 25.6 Microsoft Dynamics 365 Business Central 2023 Wave 2 – Update 23.18 Microsoft Dynamics 365 Business Central Wave 1 2024 – Update 24.12 Microsoft SharePoint Server Subscription Edition System Center Operations Manager 2025 System Center Operations Manager 2022 System Center Operations Manager 2019 System Center Service Manager 2025 System Center Service Manager 2022 System Center Service Manager 2019 System Center Orchestrator 2025 System Center Orchestrator 2022 System Center Orchestrator 2019 System Center Data Protection Manager 2019 System Center Data Protection Manager 2022 System Center Data Protection Manager 2025 System Center Virtual Machine Manager 2025 System Center Virtual Machine Manager 2019 System Center Virtual Machine Manager 2022 SharePoint Server Subscription Edition Language Pack Microsoft Office for Universal Microsoft Office for Android
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
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 15.5, 15.6 Public Cloud Module 15-SP6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Real Time Module 15-SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20251178-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20251177-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20251176-1/

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45490, CVE-2024-45491, CVE-2024-45492, CVE-2024-50602, CVE-2024-2961, CVE-2024-52533, CVE-2023-6780, CVE-2025-26466)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell iDRAC9. 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	iDRAC9 Versions prior to 7.00.00.181 iDRAC9 Versions prior to 7.20.30.50
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000299628/dsa-2025-146-security-update-for-dell-idrac9-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000299624/dsa-2025-145-security-update-for-dell-idrac9-vulnerability

Affected Product	**Ivanti**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-22464, CVE-2025-22465, CVE-2025-22466, CVE-2025-22458, CVE-2025-22459, CVE-2025-22461)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in Ivanti Endpoint Manager. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Remote Code Execution, Privilege Escalation, intercept traffic. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Endpoint Manager 2024, 2022 SU6 and previous
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-EPM-April-2025-for-EPM-2024-and-EPM-2022-SU6?language=en_US

Affected Product	**FortiGuard**	
Severity	**High**, **Medium**, **Low**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-25254, CVE-2025-22855, CVE-2024-46671, CVE-2024-32122, CVE-2024-52962, CVE-2024-26013, CVE-2024-50565, CVE-2024-54024, CVE-2024-54025)	
Description	FortiGuard has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Path Traversal, OS Command Injection, Sensitive Information Disclosure. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.	
Affected Products	FortiWeb 7.6 versions 7.6.0 through 7.6.2 FortiWeb 7.4 versions 7.4.0 through 7.4.6 FortiWeb 7.2 all versions FortiWeb 7.0 all versions FortiClientEMS 7.4 versions 7.4.0 through 7.4.1 FortiClientEMS 7.2 versions 7.2.1 through 7.2.8 FortiOS 7.4 all versions FortiOS 7.2 all versions FortiOS 7.0 all versions FortiOS 6.4 all versions FortiAnalyzer 7.6 versions 7.6.0 through 7.6.1 FortiAnalyzer 7.4 versions 7.4.0 through 7.4.5 FortiAnalyzer 7.2 versions 7.2.0 through 7.2.8 FortiAnalyzer 7.0 versions 7.0.0 through 7.0.13	FortiManager 7.6 versions 7.6.0 through 7.6.1 FortiManager 7.4 versions 7.4.0 through 7.4.5 FortiManager 7.2 versions 7.2.0 through 7.2.8 FortiManager 7.0 versions 7.0.0 through 7.0.13 FortiProxy 7.4 versions 7.4.0 through 7.4.2 FortiProxy 7.2 versions 7.2.0 through 7.2.9 FortiProxy 7.0 versions 7.0.0 through 7.0.15 FortiProxy 2.0 all versions FortiVoice 7.0 versions 7.0.0 through 7.0.2 FortiVoice 6.4 versions 6.4.0 through 6.4.8 FortiVoice 6.0 all versions FortiIsolator 2.4 versions 2.4.3 through 2.4.6 FortiIsolator 2.4 versions 2.4.3 through 2.4.6
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	• https://www.fortiguard.com/psirt/FG-IR-24-474 • https://www.fortiguard.com/psirt/FG-IR-23-344 • https://www.fortiguard.com/psirt/FG-IR-24-184 • https://www.fortiguard.com/psirt/FG-IR-24-111 • https://www.fortiguard.com/psirt/FG-IR-24-453 • https://www.fortiguard.com/psirt/FG-IR-24-046 • https://www.fortiguard.com/psirt/FG-IR-24-397 • https://www.fortiguard.com/psirt/FG-IR-24-392	

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-0064, CVE-2025-23186, CVE-2024-56337, CVE-2025-30014, CVE-2025-27428, CVE-2025-26654, CVE-2025-30013, CVE-2025-31332, CVE-2025-26657, CVE-2025-26653, CVE-2025-30017, CVE-2025-31333, CVE-2025-27437, CVE-2025-31331, CVE-2025-27435, CVE-2025-30015, CVE-2025-27430)
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, Cross-Site Scripting, Authorization Bypass, Information Disclosure, Code Injection. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP BusinessObjects Business Intelligence platform (Central Management Console), Versions - ENTERPRISE 430, 2025 • SAP NetWeaver Application Server ABAP, 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 • SAP Commerce Cloud, Versions - HY_COM 2205, COM_CLOUD 2211 • SAP Capital Yield Tax Management, Versions - CYTERP 420_700, CYT 800, IBS 7.0, CYT4HANA 100 • SAP NetWeaver and ABAP Platform (Service Data Collection), Versions - ST-PI 2008_1_700, 2008_1_710, 740 • SAP Commerce Cloud (Public Cloud), Version - COM_CLOUD 2211 • SAP ERP BW Business Content, Versions - BI_CONT 707, 737, 747, 757 • SAP BusinessObjects Business Intelligence Platform, Version - ENTERPRISE 430 • SAP KMC WPC, Version - KMC-WPC 7.50 • SAP NetWeaver Application Server ABAP (applications based on SAP GUI for HTML), 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 • SAP Solution Manager, Versions - ST 720, 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 914 • SAP S4CORE entity, Versions - S4CORE 107, 108 • SAP NetWeaver Application Server ABAP (Virus Scan Interface), Versions - 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 NetWeaver, Versions - SAP_ABA 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, 75I • SAP Commerce Cloud, Versions - HY_COM 2205, COM_CLOUD 2211 • SAP NetWeaver and ABAP Platform (Application Server ABAP), Versions - KRNL64UC 7.53, KERNEL 7.53, 7.54 • SAP CRM and SAP S/4HANA (Interaction Center), Versions - S4CRM 100, 200, 204, 205, 206, S4FND 102, 103, 104, 105, 106, 107, 108, S4CEXT 107, 108, BBPCRM 701, 702, 712, 713, 714, WEBCUIF 701, 731, 746, 747, 748, 800, 801
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html

Affected Product	**F5**
Severity	**Low**
Affected Vulnerability	Security Update (CVE-2024-4032)
Description	F5 has released security updates addressing a vulnerability that exists in BIG-IP modules. **CVE-2024-4032** - The “ipaddress” module contained incorrect information about whether certain IPv4 and IPv6 addresses were designated as “globally reachable” or “private”. This affected the is_private and is_global properties of the ipaddress.IPv4Address, ipaddress.IPv4Network, ipaddress.IPv6Address, and ipaddress.IPv6Network classes, where values wouldn’t be returned in accordance with the latest information from the IANA Special-Purpose Address Registries. CPython 3.12.4 and 3.13.0a6 contain updated information from these registries and thus have the intended behavior. 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, 17.1.0 - 17.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000150749

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.