Advisory Alert

Alert Number: AAA20260211 **Date:** February 11, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SAP	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
Dell	**High**	Improper Access Control Vulnerability
Lenovo	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
Intel	**High**, Medium	Multiple Vulnerabilities
MongoDB	**High**, Medium	Multiple Vulnerabilities
AMD	**High**, Medium, Low	Multiple Vulnerabilities
SAP	**High**, Medium, Low	Multiple Vulnerabilities
Fortinet	**High**, Medium, Low	Multiple Vulnerabilities
Red Hat	Medium	Multiple Vulnerabilities

Description

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-0488, CVE-2026-0509)
Description	SAP has released monthly security updates addressing multiple vulnerabilities that exist in their Products. **CVE-2026-0488** - An authenticated attacker in SAP CRM and SAP S/4HANA (Scripting Editor) could exploit a flaw in a generic function module call and execute unauthorized critical functionalities, which includes the ability to execute an arbitrary SQL statement. This leads to a full database compromise with high impact on confidentiality, integrity, and availability. **CVE-2026-0509** - SAP NetWeaver Application Server ABAP and ABAP Platform allows an authenticated, low-privileged user to perform background Remote Function Calls without the required S_RFC authorization in certain cases. This can result in a high impact on integrity and availability of the application. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP CRM and SAP S/4HANA (Scripting Editor) Versions (S4FND 102, 103, 104, 105, 106, 107, 108, 109, SAP_ABA 700, WEBCUIF 700, 701, 730, 731, 746, 747, 748, 800, 801) • SAP NetWeaver Application Server ABAP and ABAP Platform (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, 9.16, 9.18, 9.19)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/february-2026.html

Affected Product	**Microsoft**	
Severity	**Critical**	
Affected Vulnerability	Multiple Vulnerabilities	
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 affected systems. Microsoft advises to apply security fixes at your earliest to protect systems from potential threats.	
Affected Products	• Windows App for Mac • Windows 10 Version 1607 for x64-based Systems • Windows 10 Version 1607 for 32-bit Systems • Windows Server 2025 • Windows 11 Version 24H2 for x64-based Systems • Windows 11 Version 24H2 for ARM64-based Systems • Windows Server 2022, 23H2 Edition (Server Core installation) • Windows 11 Version 23H2 for x64-based Systems • Windows 11 Version 23H2 for ARM64-based Systems • Windows 11 Version 25H2 for x64-based Systems	• Microsoft SharePoint Server Subscription Edition • Azure HDInsight • Microsoft Defender for Endpoint for Linux • Azure AI Language Authoring • Azure IoT Explorer • Microsoft Exchange Server 2019 Cumulative Update 14 • Microsoft Exchange Server 2019 Cumulative Update 15 • Microsoft Exchange Server 2016 Cumulative Update 23 • Microsoft Exchange Server Subscription Edition RTM • Microsoft ACI Confidential Containers • Power BI Report Server • Visual Studio Code • .NET 9.0 installed on Windows • .NET 9.0 installed on Linux

	• Windows 11 Version 25H2 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 Version 22H2 for x64-based Systems • Windows 10 Version 21H2 for x64-based Systems • Windows 10 Version 21H2 for ARM64-based Systems • Windows 10 Version 21H2 for 32-bit Systems • Windows Server 2022 (Server Core installation) • Windows Server 2022 • Windows Server 2012 R2 (Server Core installation) • Windows Server 2012 R2 • Windows Server 2012 (Server Core installation) • Windows Server 2012 • Windows Server 2019 (Server Core installation) • Windows Server 2019 • Windows 10 Version 1809 for x64-based Systems • Windows 10 Version 1809 for 32-bit Systems • Windows Server 2016 (Server Core installation) • Windows Server 2016 • 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 • Microsoft SharePoint Server 2019 • Microsoft SharePoint Enterprise Server 2016 • GitHub Copilot Plugin for JetBrains IDEs • Windows 11 version 26H1 for x64-based Systems • Windows 11 Version 26H1 for ARM64-based Systems • Windows Notepad • Azure Local • Microsoft Visual Studio 2022 version 18.3 • Microsoft Visual Studio 2022 version 17.14 • Microsoft Excel 2016 (64-bit edition) • Microsoft Excel 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 • Office Online Server • Microsoft Word 2016 (64-bit edition) • Microsoft Word 2016 (32-bit edition)	• .NET 9.0 installed on Mac OS • .NET 8.0 installed on Mac OS • .NET 10.0 installed on Linux • .NET 8.0 installed on Windows • .NET 8.0 installed on Linux • .NET 10.0 installed on Windows • .NET 10.0 installed on Mac OS • Microsoft Outlook 2016 (64-bit edition) • Microsoft Outlook 2016 (32-bit edition) • Azure DevOps Server 2022 • Microsoft Edge (Chromium-based) • Azure Front Door • Azure Functions • Azure ARC • Microsoft Office 2016 (64-bit edition) • Microsoft Office 2016 (32-bit edition) • Microsoft Account • Microsoft 365 Word Copilot • Azure Logic Apps • Microsoft 365 Copilot • Microsoft Entra ID • Azure Data Explorer • Azure Resource Manager • Microsoft Copilot Studio • Microsoft Power Apps Desktop Client • 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 32-bit Systems Service Pack 2 • 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 2008 for x64-based Systems Service Pack 2 (Server Core installation) • Azure Core shared client library for Python • Windows SDK • Azure Connected Machine Agent • Microsoft Office Deployment Tool • Windows Admin Center in Azure Portal • Microsoft SQL Server 2022 for x64-based Systems (CU 22) • Microsoft SQL Server 2025 for x64-based Systems (GDR) • Microsoft SQL Server 2022 for x64-based Systems (GDR)
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/	

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Improper Access Control Vulnerability (CVE-2026-23856)
Description	Dell has released security updates addressing a vulnerability that exist in their IDRAC service module of their products. **CVE-2026-23856** - Dell iDRAC Service Module (iSM) for Windows and linux contain an Improper Access Control vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	iDRAC Service Module for Windows Versions prior to 5.4.1.1 and 6.0.3.1 iDRAC Service Module for Linux Versions prior to 5.4.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000426282/dsa-2026-077-security-update-for-dell-idrac-service-module-vulnerability

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Lenovo has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. 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-210698 https://support.lenovo.com/us/en/product_security/LEN-212143

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. HPE 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.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05010en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04992en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05008en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05007en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05006en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04999en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn05005en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05002en_us&docLocale=en_US

Affected Product	**Intel**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-32735, CVE-2025-35992, CVE-2025-33030, CVE-2025-32092, CVE-2025-32453, CVE-2025-32739, CVE-2025-32003, CVE-2025-27243, CVE-2025-24851, CVE-2025-27535, CVE-2025-32008, CVE-2025-20080, CVE-2025-27708)
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	Intel® Ethernet Adapters 800 Series Controllers and Adapters before version 30.3 or later Versions before 11.13.1: • Intel® C420 Chipset • Intel® X299 Chipset • Intel® C230 Series Chipset Version before 11.9.5: • 8th Gen Intel® Core™ processor • Intel® 200 Series Chipset • Intel® 100 Series Chipset Versions before 12.1.1: • 8th Gen Intel® Core™ processor • 9th Gen Intel® Core™ processor • Intel® 300 Series Chipset • Intel® C240 Series Chipset • Pentium® Gold processor series (G54XXU) • Celeron® processor 4000 series • Intel® 400 Series Chipset versions before 14.1.79 Versions before 15.0.55: • Intel® 500 Series Chipset • Intel® C250 Series Chipset • Intel® C740 Series Chipset versions before 15.20.25 Versions before 16.1.40: • Intel® 600 Series Chipset • Intel® 700 series chipset 5th Gen Intel® Xeon® Processor versions before 16.11.25 Intel® Core™ Ultra Processors (Series 1) versions before 18.0.18 Intel® Core™ Ultra Processors (Series 2) versions before 19.0.5 Intel® Core™ Ultra Processors (Series 2) versions before 20.0.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01403.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01385.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01171.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01315.html

Affected Product	**MongoDB**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-2303, CVE-2026-2302, CVE-2026-25613, CVE-2026-1849, CVE-2026-1850, CVE-2026-25609, CVE-2026-25610, CVE-2026-1848, CVE-2026-1847, CVE-2026-25612, CVE-2026-25611)
Description	MongoDB has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. MongoDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	MongoDB Server Versions: • 7.0 affects versions prior to 7.0.29 • 8.0 affects versions prior to 8.0.18 • 8.0 affects versions prior to 8.0.13 • 8.2 affects versions prior to 8.2.4 • 8.2 affects versions prior to 8.2.2 MongoDB Go Driver Versions: • prior to 1.17.7 • prior to 2.4.2 MongoDB Ruby Driver Versions: • 7.0.0 affects 7.6.1 and prior versions • 8.0.0 affects 8.0.12 and prior versions • 8.1.0 affects 8.1.12 and prior versions • 9.0.0 affects 9.0.10 and prior versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.mongodb.com/resources/products/alerts#security

Affected Product	**AMD**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	AMD has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. AMD 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.amd.com/en/resources/product-security/bulletin/amd-sb-4013.html • https://www.amd.com/en/resources/product-security/bulletin/amd-sb-3023.html • https://www.amd.com/en/resources/product-security/bulletin/amd-sb-6024.html

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
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 affected systems. SAP 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.sap.com/en/my-support/knowledge-base/security-notes-news/february-2026.html

Affected Product	**Fortinet**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-62676, CVE-2025-62439, CVE-2025-64157, CVE-2026-22153, CVE-2026-21743, CVE-2025-55018, CVE-2025-68686, CVE-2025-52436)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Fortinet advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiClientWindows 7.4 versions 7.4.0 through 7.4.4 FortiClientWindows 7.2 versions 7.2.0 through 7.2.12 FortiClientWindows 7.0 (7.0 all versions) FortiOS 7.6 versions 7.6.0 through 7.6.4 FortiOS 7.4 versions 7.4.0 through 7.4.9 FortiOS 7.2 (7.2 all versions) FortiOS 7.0 (7.0 all versions) FortiOS 6.4 (6.4 all versions) FortiAuthenticator 6.6 versions 6.6.0 through 6.6.6 FortiAuthenticator 6.5 (6.5 all versions) FortiAuthenticator 6.4 (6.4 all versions) FortiAuthenticator 6.3 (6.3 all versions) FortiSandbox 5.0 versions 5.0.0 through 5.0.1 FortiSandbox 4.4 versions 4.4.0 through 4.4.7 FortiSandbox 4.2 (4.2 all versions) FortiSandbox 4.0 (4.0 all versions)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.fortiguard.com/psirt/FG-IR-25-384 • https://www.fortiguard.com/psirt/FG-IR-25-795 • https://www.fortiguard.com/psirt/FG-IR-25-1052 • https://www.fortiguard.com/psirt/FG-IR-25-528 • https://www.fortiguard.com/psirt/FG-IR-25-667 • https://www.fortiguard.com/psirt/FG-IR-25-934 • https://www.fortiguard.com/psirt/FG-IR-25-093

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-50673, CVE-2022-50865, CVE-2023-53581, CVE-2023-53673, CVE-2023-53751, CVE-2023-53833, CVE-2025-39817, CVE-2025-40154, CVE-2025-40258, CVE-2025-40304, CVE-2025-40322, CVE-2025-68301, CVE-2025-68349)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the kernel of 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-2026:2490

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.