Advisory Alert

Alert Number: AAA20260114 **Date:** January 14, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SAP	**Critical**	Multiple Vulnerabilities
Fortinet	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
Lenovo	**High**	Multiple Vulnerabilities
F5	**High**	Use After Free Vulnerability
SAP	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Fortinet	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Node.js	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-0501, CVE-2026-0500, CVE-2026-0498, CVE-2026-0491)
Description	SAP has released a security update addressing multiple vulnerabilities that affect their products. These vulnerabilities could be exploited by malicious users to conduct SQL Injection, Remote Code Execution and Code Injection attacks. SAP advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• SAP S/4HANA S4CORE 102, 103, 104, 105, 106, 107, 108 and 109 • SAP Wily Introscope Enterprise Manager version WILY_INTRO_ENTERPRISE 10.8 • SAP Landscape Transformation versions DMIS 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2018_1_752 and 2020
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/january-2026.html

Affected Product	**Fortinet**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-47855, CVE-2025-64155)
Description	Fortinet has released a security update addressing multiple vulnerabilities that affect their products. **CVE-2025-47855**: An exposure of sensitive information to an unauthorized actor vulnerability in FortiFone Web Portal page may allow an unauthenticated attacker to obtain the device configuration via crafted HTTP or HTTPS requests. **CVE-2025-64155**: 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 TCP requests. Fortinet advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	FortiFone 7.0 versions 7.0.0 through 7.0.1 FortiFone 3.0 versions 3.0.13 through 3.0.23 FortiSIEM 7.4 versions 7.4.0 FortiSIEM 7.3 versions 7.3.0 through 7.3.4 FortiSIEM 7.2 versions 7.2.0 through 7.2.6 FortiSIEM 7.1 versions 7.1.0 through 7.1.8 FortiSIEM 7.0 versions 7.0.0 through 7.0.4 FortiSIEM 6.7 versions 6.7.0 through 6.7.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.fortiguard.com/psirt/FG-IR-25-260 • https://www.fortiguard.com/psirt/FG-IR-25-772

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 the affected system. Microsoft advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Windows Server 2025 (Server Core installation) • Windows Server 2025 • Windows Server 2022, 23H2 Edition (Server Core installation) • Windows Server 2022 (Server Core installation) • Windows Server 2022 • Windows Server 2019 (Server Core installation) • Windows Server 2019 • Windows Server 2016 (Server Core installation) • Windows Server 2016 • 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 SDK • Windows Admin Center in Azure Portal • Windows 11 Version 25H2 for x64-based Systems • Windows 11 Version 25H2 for ARM64-based Systems • Windows 11 Version 24H2 for x64-based Systems • Windows 11 Version 24H2 for ARM64-based Systems • Windows 11 Version 23H2 for x64-based Systems • Windows 11 Version 23H2 for ARM64-based Systems • Windows 10 Version 22H2 for x64-based Systems • Windows 10 Version 22H2 for ARM64-based Systems • Windows 10 Version 22H2 for 32-bit 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 10 Version 1809 for x64-based Systems • Windows 10 Version 1809 for 32-bit Systems • Windows 10 Version 1607 for x64-based Systems • Windows 10 Version 1607 for 32-bit Systems • Office Online Server • Microsoft Word 2016 (64-bit edition) • Microsoft Word 2016 (32-bit edition)	• Microsoft SQL Server 2025 for x64-based Systems (GDR) • Microsoft SQL Server 2022 for x64-based Systems (GDR) • Microsoft SQL Server 2022 for x64-based Systems (CU 22) • Microsoft SharePoint Server Subscription Edition • Microsoft SharePoint Server 2019 • Microsoft SharePoint Enterprise Server 2016 • Microsoft Office LTSC for Mac 2024 • Microsoft Office LTSC for Mac 2021 • Microsoft Office LTSC 2024 for 64-bit editions • Microsoft Office LTSC 2024 for 32-bit editions • Microsoft Office LTSC 2021 for 64-bit editions • Microsoft Office LTSC 2021 for 32-bit editions • Microsoft Office Deployment Tool • Microsoft Office 2019 for 64-bit editions • Microsoft Office 2019 for 32-bit editions • Microsoft Office 2016 (64-bit edition) • Microsoft Office 2016 (32-bit edition) • Microsoft Excel 2016 (64-bit edition) • Microsoft Excel 2016 (32-bit edition) • Microsoft Edge (Chromium-based) • Microsoft 365 Apps for Enterprise for 64-bit Systems • Microsoft 365 Apps for Enterprise for 32-bit Systems • cbl2 ruby 3.1.7-3 • cbl2 reaper 3.1.1-22 • cbl2 python-tensorboard 2.11.0-3 • cbl2 nmap 7.93-3 • cbl2 libsodium 1.0.18-6 • cbl2 libpcap 1.10.1-4 • cbl2 kernel 5.15.186.1-1 • Azure Core shared client library for Python • Azure Connected Machine Agent • azl3 ruby 3.3.5-6 • azl3 python-tensorboard 2.16.2-6 • azl3 nmap 7.95-2 • azl3 libtpms 0.9.6-8 • azl3 libsodium 1.0.19-1 • azl3 libpcap 1.10.5-1 • azl3 libcap 2.69-10 • azl3 kernel 6.6.117.1-1 • azl3 net-snmp 5.9.4-1 • cbl2 net-snmp 5.9.4-1 • Office Out-of-Box Experience • Azure Cosmos DB • Microsoft Purview • Azure Container Apps • Microsoft Partner Center • Azure Cognitive Service for Language • Microsoft Office for Android
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38051, CVE-2023-53322, CVE-2023-53401, CVE-2025-39898, CVE-2023-53513, CVE-2023-53680, CVE-2022-50543, CVE-2023-53675, CVE-2025-39971, CVE-2025-68285, CVE-2025-39825, CVE-2025-39817, CVE-2025-39883, CVE-2025-39993, CVE-2023-53705, CVE-2025-38724, CVE-2025-23142, CVE-2025-39982, CVE-2025-40141, CVE-2025-40176, CVE-2025-68287)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Red Hat advises to apply these security fixes at your earliest to protect your 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 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.4 x86_64 Red Hat Enterprise Linux Server - AUS 8.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64 Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:0536 • https://access.redhat.com/errata/RHSA-2026:0533 • https://access.redhat.com/errata/RHSA-2026:0532 • https://access.redhat.com/errata/RHSA-2026:0489

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-37181, CVE-2026-37182, CVE-2026-37183, CVE-2026-37184, CVE-2026-37185, CVE-2025-37186, CVE-2025-37168, CVE-2025-37169, CVE-2025-37170, CVE-2025-37171, CVE-2025-37172, CVE-2025-37173, CVE-2025-37174, CVE-2025-37175, CVE-2025-37176, CVE-2025-37177, CVE-2025-37178, CVE-2025-37179, CVE-2025-37165, CVE-2025-37166, CVE-2023-52340, CVE-2022-48839)
Description	HPE has released a security update addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to conduct Cross Site Scripting (XSS), SQL Injection, Access Restriction Bypass, Arbitrary Command Execution and Denial of Service attacks. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	EdgeConnect SD-WAN Orchestrator version 9.6.x: 9.6.0 EdgeConnect SD-WAN Orchestrator version 9.5.x: 9.5.5 and below EdgeConnect SD-WAN Orchestrator version 9.4.x: 9.4.4 and below Mobility Conductors Mobility Controllers WLAN and SD-WAN Gateways Managed by HPE Aruba Networking Central AOS-10.7.x.x: 10.7.2.1 and below AOS-10.4.x.x: 10.4.1.9 and below AOS-8.13.x.x: 8.13.1.0 and below AOS-8.10.x.x: 8.10.0.20 and below HPE Networking Instant On devices running software version 3.3.1.0 and below • HPE Aruba Networking VIA client for Linux: ○ Version 4.7.5 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04992en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04994en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04987en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04988en_us&docLocale=en_US

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-27053, CVE-2025-12050, CVE-2025-12051, CVE-2025-47348, CVE-2026-0421)
Description	Lenovo has released a security update addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to conduct Privilege Escalation, Arbitrary Code Execution and Memory Corruption attacks. Lenovo advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	ThinkPad T14s Gen 6 (Type 21N1, 21N2) versions prior to 1.0.4338.2200 ThinkPad X13s Gen 1 (Type 21BX, 21BY) versions prior to 1.0.4195.6500 IdeaPad 5x 2-in-1 (14-Inch) (83GH) versions prior to 1.0.4458.2600 ThinkBook 16 G7 QOY (21NH) versions prior to 1.0.4458.2600 IdeaPad Slim 5x (14-Inch) (83HL) versions prior to 1.0.4374.1300 IdeaPad Slim 3 15Q8X10 versions prior to 1.0.4458.2600 Lenovo Yoga Slim 7 14Q8X9 (83ED) versions prior to 1.0.4374.1300 L13 2-in-1 Gen 6 (Type 21R7, 21R8) Laptops (ThinkPad) versions prior to 1.36 L13 Gen 6 (Type 21R5, 21R6) Laptops (ThinkPad) versions prior to 1.36 L14 Gen 6 (Type 21S6, 21S7) Laptops (ThinkPad) versions prior to 1.06 L16 Gen 2 (Type 21SA, 21SB) Laptops (ThinkPad) versions prior to1.06 S2 2 in 1 Gen 10 (Type 21RA) China Only Laptops (ThinkPad) versions prior to 1.36 S2 Gen 10 Type 21R9 China Only Laptops (ThinkPad) versions prior to 1.36
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.lenovo.com/us/en/product_security/ps500790-qualcomm-driver-vulnerability • https://support.lenovo.com/sa/en/product_security/ps500793-multi-vendor-bios-security-vulnerabilities-january-2026

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Use After Free Vulnerability (CVE-2025-49844)
Description	F5 has released a security update addressing multiple vulnerabilities that exists in their products. **CVE-2025-49844**: This vulnerability allows an authenticated user to use a specially crafted Lua script to manipulate the garbage collector, trigger a use-after-free and potentially lead to remote code execution. F5 advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	BIG-IP Next SPK versions 2.0.0 to 2.0.2 and 1.7.0 to 1.9.2 BIG-IP Next CNF versions 2.0.0 to 2.1.0 and 1.1.0 to 1.4.1 BIG-IP Next for Kubernetes versions 2.0.0 to 2.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000159544

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-0492, CVE-2026-0507, CVE-2026-0511, CVE-2026-0496, CVE-2026-0495, CVE-2026-0506, CVE-2026-0503, CVE-2026-0499, CVE-2026-0514, CVE-2026-0513, CVE-2026-0494, CVE-2026-0493, CVE-2026-0497, CVE-2026-0504, CVE-2026-0510)
Description	SAP has released a security update addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to conduct Privilege Escalation, OS Command Injection, Cross-Site Scripting (XSS), and Information Disclosure. SAP advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• SAP HANA database version HDB 2.00 • SAP Application Server for ABAP and SAP NetWeaver RFCSDK versions KRNL64UC 7.53, NWRFCSDK 7.50, KERNEL 7.53, 7.54, 7.77, 7.89, 7.93, 9.16 • SAP Fiori App versions UIAPFI70 500, 600, 700, 800, 900, 901, 902, S4CORE 102, 103, 104, 105, 106, 107, 108, 109, UIS4H 109 • SAP NetWeaver Application Server ABAP and ABAP Platform 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_BASIS 816 • SAP ERP Central Component and SAP S/4HANA versions SAP_APPL 618, S4CORE 102, 103, 104, 105, 106, 107, 108, 109, EA-APPL 605, 606, 617 • SAP NetWeaver Enterprise Portal version EP-RUNTIME 7.50 • SAP Business Connector versions SAP BC 4.8 • SAP Supplier Relationship Management versions SRM_SERVER 700, 701, 702, 713, 714 • Business Server Pages Application versions SAP_APPL 618, S4CORE 102, 103, 104, 105, 106, 107, 108, 109, EA-APPL 600, 602, 603, 604, 605, 606, 617 • SAP Identity Management versions IDM_CLM_REST_API 8.0, IDMIC 8.0 • NW AS Java UME User Mapping versions ENGINEAPI 7.50, SERVERCORE 7.50, UMEADMIN 7.50
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/january-2026.html

Affected Product	**Fortinet**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-25249, CVE-2025-59922, CVE-2025-67685)
Description	Fortinet has released a security update addressing multiple vulnerabilities that exists in their products. **CVE-2025-25249**: A heap-based buffer overflow vulnerability in FortiOS and FortiSwitchManager cw_acd daemon may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests. **CVE-2025-59922**: An improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in FortiClientEMS may allow an authenticated attacker with at least read-only admin permission to execute unauthorized SQL code or commands via crafted HTTP or HTTPs requests. **CVE-2025-67685**: A Server-Side Request Forgery (SSRF) vulnerability in FortiSandbox may allow an authenticated attacker to proxy internal requests limited to plaintext endpoints only via crafted HTTP requests. Fortinet advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	FortiOS 7.6 versions 7.6.0 through 7.6.3 FortiOS 7.4 versions 7.4.0 through 7.4.8 FortiOS 7.2 versions 7.2.0 through 7.2.11 FortiOS 7.0 versions 7.0.0 through 7.0.17 FortiOS 6.4 versions 6.4.0 through 6.4.16 FortiSASE 25.1.a versions 25.1.a.2 FortiSwitchManager 7.2 versions 7.2.0 through 7.2.6 FortiSwitchManager 7.0 versions 7.0.0 through 7.0.5 FortiClientEMS 7.4 versions 7.4.3 through 7.4.4 FortiClientEMS 7.4 versions 7.4.0 through 7.4.1 FortiClientEMS 7.2 versions 7.2.0 through 7.2.10 FortiClientEMS 7.0 versions 7.0 all versions FortiSandbox 5.0 versions 5.0.0 through 5.0.4 FortiSandbox 4.4 versions 4.4 all versions FortiSandbox 4.2 versions 4.2 all versions FortiSandbox 4.0 versions 4.0 all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.fortiguard.com/psirt/FG-IR-25-084 • https://www.fortiguard.com/psirt/FG-IR-25-735 • https://www.fortiguard.com/psirt/FG-IR-25-783

Affected Product	**Node.js**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-55131, CVE-2025-55130, CVE-2025-59465, CVE-2025-59466, CVE-2025-59464, CVE-2026-21636, CVE-2026-21637, CVE-2025-55132)
Description	Node.js has released a security update addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to conduct Memory Corruption, File System Permission Bypass, Denial of Service (DoS), Privilege Escalation and Code Execution. Node.js advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Node.js versions • 25.x • 24.x • 22.x • 20.x Dependencies • c-ares (1.34.6) on versions 20.x, 22.x, 24.x, 25.x • undici (6.23.0, 7.18.0) on versions 20.x, 22.x, 24.x, 25.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nodejs.org/en/blog/vulnerability/december-2025-security-releases

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.