Advisory Alert

Alert Number: AAA20260513 **Date:** May 13, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortinet	**Critical**	Multiple Vulnerabilities
Ivanti	**Critical**	Security Update
Microsoft	**Critical**	Multiple Vulnerabilities
SAP	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Lenovo	**High**	Multiple Vulnerabilities
Barracuda	**High**	Privilege Escalation Vulnerabilities
Ivanti	**High, Medium**	Multiple Vulnerabilities
Intel	**High, Medium**	Multiple Vulnerabilities
HPE	**High, Medium**	Multiple Vulnerabilities
SAP	**High, Medium, Low**	Multiple Vulnerabilities
AMD	**High, Medium, Low**	Multiple Vulnerabilities
Fortinet	**High, Medium, Low**	Multiple Vulnerabilities
IBM	**High, Medium, Low**	Multiple Vulnerabilities
HP	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Fortinet**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-44277, CVE-2026-26083)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-44277:** An Improper Access Control vulnerability in FortiAuthenticator may allow an unauthenticated attacker to execute unauthorized code or commands via crafted requests. **CVE-2026-26083:** A missing authorization vulnerability in FortiSandbox, FortiSandbox Cloud and FortiSandbox PaaS WEB UI may allow an unauthenticated attacker to execute unauthorized code or commands via HTTP requests. Fortinet advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiAuthenticator 8.0 – Versions 8.0.0 & 8.0.2 FortiAuthenticator 6.6 – Versions 6.6.0 through 6.6.8 FortiAuthenticator 6.5 – Versions 6.5.0 through 6.5.6 FortiSandbox 5.0 – Versions 5.0.0 through 5.0.1 FortiSandbox 4.4 – Versions 5 4.4.0 through 4.4.8 FortiSandbox Cloud 24 – All versions FortiSandbox Cloud 23 – All versions FortiSandbox Cloud 5.0 – Versions 5.0.2 through 5.0.5 FortiSandbox PaaS 23.4 – All Versions FortiSandbox PaaS 23.3 – All Versions FortiSandbox PaaS 23.1 – All Versions FortiSandbox PaaS 22.2 – All Versions FortiSandbox PaaS 22.1 – All Versions FortiSandbox PaaS 21.4 – All Versions FortiSandbox PaaS 21.3 – All Versions FortiSandbox PaaS 5.0 – Versions 5.0.0 through 5.0.1 FortiSandbox PaaS 4.4 – Versions 4.4.5 through 4.4.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.fortiguard.com/psirt/FG-IR-26-136 • https://www.fortiguard.com/psirt/FG-IR-26-128

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2026-8043)
Description	Ivanti has released a security updates addressing a vulnerability that exists in their product. **CVE-2026-8043:** External control of a file name in Ivanti Xtraction before version 2026.2 allows a remote authenticated attacker to read sensitive files and write arbitrary HTML files to a web directory, leading to information disclosure and possible client-side attacks. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Xtraction – Versions 2026.1 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://hub.ivanti.com/s/article/Security-Advisory---Ivanti-Xtraction-CVE-2026-8043?language=en_US

Affected Product	**Microsoft**	
Severity	**Critical**	
Affected Vulnerability	Multiple Vulnerabilities	
Description	Microsoft has released security update addressing multiple vulnerabilities that exists 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	ASP.NET Core Microsoft Dynamics 365 (on-premises) Windows DWM Core Library M365 Copilot Microsoft Edge (Chromium-based) Microsoft Office Azure Monitor Agent Windows Telephony Service Azure Logic Apps M365 Copilot for Desktop Visual Studio Code GitHub Copilot and Visual Studio Microsoft SSO Plugin for Jira & Confluence Microsoft Office PowerPoint Microsoft Office Word Windows Secure Boot Microsoft Windows DNS Data Deduplication Microsoft Data Formulator Windows Netlogon Windows Ancillary Function Driver for WinSock Windows Admin Center Microsoft Office Click-To-Run Dynamics Business Central Windows TCP/IP Windows SMB Client Windows Kernel-Mode Drivers Windows Common Log File System Driver Windows Win32K - GRFX Windows Hyper-V Windows Remote Desktop Azure Connected Machine Agent Windows Volume Manager Extension Driver Windows Cryptographic Services Power Automate SQL Server Windows Kernel Microsoft Office SharePoint Microsoft Office Excel .NET Microsoft Edge for Android Windows Internet Key Exchange (IKE) Protocol Telnet Client Windows GDI Windows Cloud Files Mini Filter Driver Windows Win32K - ICOMP Windows Storage Spaces Controller Windows Storport Miniport Driver Windows Application Identity (AppID) Subsystem Windows Print Spooler Components Windows Link-Layer Discovery Protocol (LLDP) Windows Projected File System Windows LDAP - Lightweight Directory Access Protocol Windows Message Queuing Windows Event Logging Service Azure Machine Learning Windows Snipping Tool Windows Active Directory Microsoft Defender Windows IKE Extension Azure SDK .NET, .NET Framework, Visual Studio Windows Container Isolation FS Filter Driver Windows HTTP.sys .NET Framework	Windows Shell Windows Server Update Service Windows USB Print Driver Microsoft Graphics Component Windows Virtualization-Based Security (VBS) Enclave Microsoft Brokering File System Windows Redirected Drive Buffering Universal Plug and Play (upnp.dll) Windows Filtering Platform (WFP) .NET and Visual Studio Microsoft Teams Microsoft High Performance Compute Pack (HPC) Microsoft Windows Windows Rich Text Edit Control Windows User Interface Core Windows COM Windows Native WiFi Miniport Driver Windows Push Notifications Remote Desktop Client Windows Universal Plug and Play (UPnP) Device Host Desktop Window Manager Microsoft Windows Speech Function Discovery Service (fdwsd.dll) Role: Windows Hyper-V Windows Speech Brokered Api Windows Biometric Service Windows Remote Procedure Call Windows File Explorer Windows SSDP Service Windows WalletService Windows Local Security Authority Subsystem Service (LSASS) Windows LUAFV Windows Hello Windows WFP NDIS Lightweight Filter Driver (wfplwfs.sys) Microsoft Management Console Windows BitLocker Windows Kerberos Windows Installer Microsoft Windows Search Component Windows TDI Translation Driver (tdx.sys) Windows RPC API Windows Advanced Rasterization Platform Windows Client Side Caching driver (csc.sys) Windows Boot Manager Microsoft PowerShell Windows Kernel Memory Windows OLE Windows Sensor Data Service Windows Remote Desktop Licensing Service Windows Encrypting File System (EFS) Microsoft Power Apps Applocker Filter Driver (applockerfltr.sys) GitHub Copilot and Visual Studio Code Windows Rich Text Edit Windows Management Services Windows Recovery Environment Agent Windows Notepad App Windows Boot Loader Servicing Stack Updates Mariner GitHub Repo: Git for Windows Node.js AMD CPU Branch Input-Output Memory Management Unit (IOMMU)
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/	

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-34260, CVE-2026-34263)
Description	SAP has released security updates addressing multiple vulnerabilities that exists in their products. **CVE-2026-34260:** SAP S/4HANA (SAP Enterprise Search for ABAP) contains a SQL injection vulnerability that allows an authenticated attacker to inject malicious SQL statements through user-controlled input. The application directly concatenates this malicious user input into SQL queries, which are then passed to the underlying database without proper validation or sanitization. Upon successful exploitation, an attacker may gain unauthorized access to sensitive database information and could potentially crash the application. **CVE-2026-34263:** Due to improper Spring Security configuration, SAP Commerce cloud allows an unauthenticated user to perform malicious configuration upload and code injection, resulting in arbitrary server-side code execution, leading to high impact on Confidentiality, Integrity, and Availability of the application. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP S/4HANA (SAP Enterprise Search for ABAP): Version(s) - 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 Commerce cloud: Version(s) - HY_COM 2205, COM_CLOUD 2211, 2211-JDK21
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2026.html

ffected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-43284, CVE-2026-31431)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exists in their products. **CVE-2026-43284:** The “Dirty Frag” vulnerability is a local privilege escalation (LPE) issue in the Linux kernel that combines flaws in the ESP/XFRM and RXRPC subsystems to allow an unprivileged local attacker to gain root access on major Linux distributions (using any of these two: ESP/XFRM or RXRPC flaws). The attack abuses kernel page-cache manipulation and network protocol handling to overwrite privileged binaries and execute arbitrary code with elevated privileges. **CVE-2026-31431:** A flaw was found in the Linux kernel's algif_aead cryptographic algorithm interface. An incorrect 'in-place operation' was introduced, where the source and destination data mappings were different. This could lead to unexpected behavior or data integrity issues during cryptographic operations, potentially impacting the reliability of encrypted communications. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 & 10.0 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x & 10.0 s390x Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 & 10.0 x86_64 Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2, 9.6 & 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.2 & 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 & 10.0 aarch64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x, 9.6 s390x & 10.0 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.2 s390x & 9.6 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x & 10.0 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.2 ppc64le & 9.6 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le & 10.0 ppc64le Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.2 x86_64 & 9.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 & 10.0 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 & AUS 9.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:16206 https://access.redhat.com/errata/RHSA-2026:16312 https://access.redhat.com/errata/RHSA-2026:16314 https://access.redhat.com/errata/RHSA-2026:16328 https://access.redhat.com/errata/RHSA-2026:16209 https://access.redhat.com/errata/RHSA-2026:16210

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-27723, CVE-2024-36315, CVE-2025-61971, CVE-2025-61972)
Description	Dell has released security update 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 Servers (BIOS): • PowerEdge R6715 / R7715 / R6725 / R7725 / M7725 / XE7745 - Versions prior to 1.6.4 • PowerEdge R7725xd - Versions prior to 1.6.5 • PowerEdge XE9785 - Versions prior to 1.1.4 • PowerEdge XE9785L - Versions prior to 1.2.1 • PowerEdge R6615 / R7615 / R6625 / R7625 / XC Core XC7625 - Versions prior to 1.16.2 • PowerEdge C6615 - Versions prior to 1.11.2 • PowerEdge XE9685L - Versions prior to 1.3.4 • PowerEdge R6515 / R6525 / R7515 / R7525 / C6525 / Dell EMC XC Core XC7525 - Versions prior to 2.23.1 • PowerEdge XE8545 - Versions prior to 2.21.0 Dell PowerEdge Software: • PowerEdge XE9680 - Versions prior to 01.25.03.12.76 • PowerEdge R7615 / R7625 / R760XA / R7515 / R7525 / R750XA - Versions prior to 1.0 Network Adapters: • Intel 800 Series Ethernet Adapters - Versions prior to 30.5.0.13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000464069/dsa-2026-076-security-update-for-dell-amd-based-poweredge-server-vulnerability • https://www.dell.com/support/kbdoc/en-us/000464090/dsa-2026-218-dell-poweredge-server-security-update-for-intel-800-series-ethernet-adapters-and-intel-data-center-gpu-vulnerabilities

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-26380, CVE-2021-46747, CVE-2022-23826, CVE-2023-31316, CVE-2024-36315, CVE-2024-36343, CVE-2024-36345, CVE-2025-0040, CVE-2025-35979, CVE-2025-35991, CVE-2025-48516, CVE-2025-54518, CVE-2025-61971, CVE-2025-61972, CVE-2026-0438)
Description	Lenovo has released a security update 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-216977

Affected Product	**Barracuda**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerabilities (CVE-2026-43284, CVE-2026-43500)
Description	Barracuda has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-43284:** The Linux kernel has been updated to prevent in-place decryption on shared socket buffer (skb) fragments in the XFRM ESP subsystem. Previously, the IPv4/IPv6 datagram paths failed to set the SKBFL_SHARED_FRAG flag when using MSG_SPLICE_PAGES, causing ESP to incorrectly decrypt data in place on memory still shared with external pipes. The fix ensures these fragments are correctly flagged, forcing ESP input to utilize skb_cow_data() to create private copies before decryption. This change secures externally backed fragments while maintaining the existing fast path for private nonlinear fragments and leaving ESP output logic unchanged, as it already handles nonlinear buffers safely. **CVE-2026-43500:** The Linux kernel has been updated to prevent in-place decryption on shared data and response packets within the rxrpc protocol. Previously, packets were only unshared if the socket buffer was cloned, allowing externally-owned paged fragments—such as those created via splice()—to bypass security safeguards and undergo in-place decryption. The fix extends the unsharing requirement to include any buffer with a fragment list or shared fragments, effectively closing the splice-loopback vulnerability. This adjustment ensures that externally-shared fragments are safely copied to linear buffers before processing while preserving the zero-copy fast path for private kernel fragments. Barracuda advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Barracuda Appliances (Physical & Virtual)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://trust.barracuda.com/security/information/linux-kernel-local-privilege-escalation-vulnerabilities-dirty-frag-copyfail2

Affected Product	**Ivanti**
Severity	**High,** **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-8051, CVE-2026-7431, CVE-2026-7432, CVE-2026-8109, CVE-2026-8110, CVE-2026-8111)
Description	Ivanti has released security update addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Virtual Traffic Manager (vTM) – Versions 22.9r3 and prior Ivanti Secure Access Client (Windows) – Versions 22.8R5 and prior Ivanti Endpoint Manager (EPM) – Versions 2024 SU5 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Virtual-Traffic-Manager-vTM-CVE-2026-8051?language=en_US • https://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Secure-Access-Client-CVE-2026-7431-CVE-2026-7432?language=en_US • https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-EPM-May-2026?language=en_US

Affected Product	**Intel**
Severity	**High,** **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-27723, CVE-2026-20753, CVE-2026-20754, CVE-2026-20718, CVE-2025-35979, CVE-2025-35991, CVE-2025-35969)
Description	Intel has released security update addressing multiple vulnerabilities that exists 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 Xeon Series • Intel Xeon Scalable: 4th and 5th Generation Intel Xeon Scalable processors Intel Xeon D Series: • Intel Xeon D-1700 and D-2700 processors • Intel Xeon D-1800 and D-2800 processors Intel Xeon Processor D Family • Intel Xeon E Series: Intel Xeon Processor E Family • Intel Xeon W Series: Intel Xeon W-11155MLE/MRE, W-11555MLE/MRE, and W-11865MLE/MRE • Intel Xeon SoC: 6700P-B/6500P-B Series SoC with P-Cores Intel Core & Ultra Series • Intel Core Ultra: • Series 3: Panther Lake (H 4P+8E+4LP_E+12Xe - C06C2) • Series 2: Lunar Lake (B06D1) • 200S Series: Arrow Lake (C0662, C0652) • Intel Core Ultra Family Intel Core (Generational): • 13th Generation Intel Core Processor Family • 12th Generation Intel Core Processor Family • 11th Generation Intel Core Processor Family (including i3-1115GRE/G4E, i5-1145G7E/GRE, i7-1185G7E/GRE, i3-11100HE, i5-11500HE, and i7-11850HE) • 10th Generation Intel Core Processor Family Intel Atom, Pentium & Celeron • Intel Atom: • P6000 Processors • Processor C5100, C5300, P5300, and P5700 • Processor E3900 Series Intel Pentium: Pentium Gold Processor Family • Intel Celeron: • Celeron Processor Family • Celeron 6305E/RE • Celeron 6600HE/HLE Software, Drivers & Firmware • Intel NPU Drivers: • Driver for Linux (v1.26.0) • Driver for Windows (v32.0.100.4511) • Utility Software: Intel Server Firmware Update Utility Software (versions prior to 16.0.12)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01426.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01425.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01424.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01420.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01413.html • https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01410.html

Affected Product	**HPE**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-35991, CVE-2026-23819, CVE-2026-23820, CVE-2026-23821, CVE-2026-23822, CVE-2026-23823, CVE-2026-23824, CVE-2026-23825, CVE-2026-23826, CVE-2026-23827, CVE-2026-44852, CVE-2026-44853, CVE-2026-44854, CVE-2026-44855, CVE-2026-44856, CVE-2026-44857, CVE-2026-44858, CVE-2026-44859, CVE-2026-44860, CVE-2026-44861, CVE-2026-44862, CVE-2026-44863, CVE-2026-44864, CVE-2026-44865, CVE-2026-44866, CVE-2026-44867, CVE-2026-44868, CVE-2026-44869, CVE-2026-44870, CVE-2026-44872, CVE-2026-44873, CVE-2026-44874)
Description	HPE has released security update addressing multiple vulnerabilities that exists 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	HPE Aruba Networking: Mobility Conductors, Mobility Controllers & WLAN and SD-WAN Gateways Managed by HPE Aruba Networking Central • AOS-10.8.x.x: 10.8.0.0 and below • AOS-10.7.x.x: 10.7.2.2 and below • AOS-10.4.x.x: 10.4.1.10 and below • AOS-8.13.x.x: 8.13.1.1 and below • AOS-8.12.x.x: 8.12.0.6 and below • AOS-8.10.x.x: 8.10.0.21 and below Access Point Running AOS-8 Instant & AOS-10 AP • AOS-10 AP 10.8.x.x: 10.8.0.0 • AOS-10 AP 10.7.x.x: 10.7.2.2 and below • AOS-10 AP 10.4.x.x: 10.4.1.10 and below • AOS-8 Instant 8.13.x.x: 8.13.1.1 and below • AOS-8 Instant 8.12.x.x: 8.12.0.6 and below • AOS-8 Instant 8.10.x.x: 8.10.0.21 and below HPE Servers & Storage (Gen11): Prior to 2.80_01-29-2026 • HPE Alletra 4110, HPE Alletra 4120 & HPE Alletra 4140 HPE ProLiant • HPE ProLiant DL110 Gen11 - Prior to 2.80_01-29-2026 • HPE ProLiant DL320 Gen11 Server - Prior to 2.80_01-29-2026 • HPE ProLiant DL360 Gen11 Server - Prior to 2.80_01-29-2026 • HPE ProLiant DL380 Gen11 Server - Prior to 2.80_01-29-2026 • HPE ProLiant DL380a Gen11 - Prior to 2.80_01-29-2026 • HPE ProLiant DL560 Gen11 - Prior to 2.80_01-29-2026 • HPE ProLiant ML110 Gen11 - Prior to 2.80_01-29-2026 • HPE ProLiant ML350 Gen11 Server - Prior to 2.80_01-29-2026 • HPE Synergy 480 Gen11 Compute Module - Prior to 2.80_01-29-2026 • HPE Compute Edge Server e930t - Prior to 2.80_01-29-2026
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05048en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05049en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05052en_us&docLocale=en_US

Affected Product	**SAP**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-34259, CVE-2026-40135, CVE-2026-40133, CVE-2026-40137, CVE-2026-0502, CVE-2026-40132, CVE-2025-68161, CVE-2026-34258, CVE-2026-27682, CVE-2026-40136, CVE-2026-40134, CVE-2026-40129, and CVE-2026-40131)
Description	SAP has released a security update addressing a vulnerability 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	• SAP Forecasting & Replenishment - Versions SCM 702, 712, 713, 714 • SAP NetWeaver Application Server for ABAP and ABAP Platform - Versions SAP_BASIS 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 758, 816 • SAP Application Server ABAP for SAP NetWeaver and ABAP Platform - Versions SAP_BASIS 740, 750, 751, 752, 753, 754, 755, 756, 757, 758, 816 • SAP NetWeaver Application Server ABAP (Applications based on Business Server Pages) - Versions SAP_BASIS 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 758, 816, 918 • SAP S/4HANA Condition Maintenance - Versions S4CORE 102, 103, 104, 105, 106, 107, 108, 109 • SAP Incentive and Commission Management - Versions SAP_APPL 618, S4CORE 102 through 109, EA-APPL 600, 604, 605, 606, 617 • SAP Strategic Enterprise Management (BSP application Balanced Scorecard Wizard) - Versions SEM-BW 605, 700, 736, 746, 747, 748, 749, 800 • Business Server Pages Application (TAF_APPLAUNCHER) - Versions ST-PI 740, 758 • SAP BusinessObjects Business Intelligence Platform - Versions ENTERPRISE 430, 2025, 2027 • SAP Commerce Cloud (Apache Log4j) - Versions HY_COM 2205, COM_CLOUD 2211, 2211-JDK21 • SAPUI5 (Search UI) - Versions SAPUI5 1.108, 1.120, 1.136, 1.142, 1.71, 1.84, 1.96 • SAP Financial Consolidation - Versions FINANCE 1010 • SAP HANA Deployment Infrastructure (HDI) deploy library - Versions XS_HDI_DEPLOYER 1.00
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2026.html

Affected Product	**AMD**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-26380, CVE-2021-46747, CVE-2022-23826, CVE-2023-31316, CVE-2024-21962, CVE-2024-36315, CVE-2024-36343, CVE-2024-36345, CVE-2025-0028, CVE-2025-0040, CVE-2025-0045, CVE-2025-29935, CVE-2025-29936, CVE-2025-29937, CVE-2025-29938, CVE-2025-29944, CVE-2025-38234, CVE-2025-48512, CVE-2025-48513, CVE-2025-48516, CVE-2025-48519, CVE-2025-48520, CVE-2025-48521, CVE-2025-52540, CVE-2025-54518, CVE-2025-61971, CVE-2025-61972, CVE-2026-0432, CVE-2026-0438)
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 Product
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-3030.html https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7052.html https://www.amd.com/en/resources/product-security/bulletin/amd-sb-4015.html https://www.amd.com/en/resources/product-security/bulletin/amd-sb-4017.html https://www.amd.com/en/resources/product-security/bulletin/amd-sb-4016.html https://www.amd.com/en/resources/product-security/bulletin/amd-sb-3047.html

Affected Product	**Fortinet**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-53680, CVE-2025-53681, CVE-2025-53844, CVE-2025-53870, CVE-2025-67604, CVE-2026-25088, CVE-2026-25690, CVE-2026-44278, CVE-2026-44279)
Description	Fortinet has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. 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 • 7.4: Versions 7.4.0 through 7.4.8 • 7.2: Versions 7.2.0 through 7.2.11 FortiNDR • 7.6: Versions 7.6.0 through 7.6.2 • 7.4: Versions 7.4.0 through 7.4.9 • 7.2 / 7.1 / 7.0: All Versions FortiManager • 7.6: Versions 7.6.0 through 7.6.4 • 7.4: Versions 7.4.0 through 7.4.8 • 7.2: All Versions FortiAnalyzer • 7.6: Versions 7.6.0 through 7.6.4 • 7.4: Versions 7.4.0 through 7.4.8 • 7.2: All Versions FortiAP • 7.6: Versions 7.6.0 through 7.6.2 • 7.4: Versions 7.4.0 through 7.4.5 • 7.2 / 6.4: All Versions FortiAP-W2 • 7.4: Versions 7.4.0 through 7.4.4 • 7.2: Versions 7.2.0 through 7.2.5 (or All Versions) FortiAP-U • 7.0: Versions 7.0.0 through 7.0.5 FortiDeceptor • 6.0: Versions 6.0.0 through 6.0.2 • 5.3: Versions 5.3.0 through 5.3.3 • 5.2: Versions 5.2.0 through 5.2.1 • 5.1 / 5.0: All Versions FortiMail • 7.6: Versions 7.6.0 through 7.6.3 • 7.4: Versions 7.4.0 through 7.4.5 • 7.2: Versions 7.2.0 through 7.2.8 FortiClient (Windows) • 7.4: Versions 7.4.0 through 7.4.2 • 7.2: All Versions FortiToken (Android) • 6.2 / 6.1 / 5.2: All Versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-26-138 https://www.fortiguard.com/psirt/FG-IR-26-131 https://www.fortiguard.com/psirt/FG-IR-26-137 https://www.fortiguard.com/psirt/FG-IR-26-129 https://www.fortiguard.com/psirt/FG-IR-26-133 https://www.fortiguard.com/psirt/FG-IR-26-130 https://www.fortiguard.com/psirt/FG-IR-26-123 https://www.fortiguard.com/psirt/FG-IR-26-132 https://www.fortiguard.com/psirt/FG-IR-26-134

Affected Product	**IBM**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3219, CVE-2025-30258, CVE-2023-50495, CVE-2025-1632, CVE-2025-5915, CVE-2025-5916, CVE-2025-5917, CVE-2025-5918, CVE-2023-32636, CVE-2025-3360, CVE-2025-4598, CVE-2025-23419, CVE-2025-5278, CVE-2025-5318, CVE-2025-5351, CVE-2025-5372, CVE-2025-5987, CVE-2025-8114, CVE-2022-27943, CVE-2022-41409, CVE-2023-4156, CVE-2024-0232, CVE-2024-13176, CVE-2026-31431)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Cloud Pak for Data System – Cyclops – Versions 11.3.0.2-IF2 IBM Storage Scale System – Versions 6.1.0.0 - 6.1.9.8 IBM Storage Scale System – Versions 6.2.0.0 - 6.2.3.5 IBM Storage Scale System – Versions 7.0.0.0 - 7.0.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7272714 • https://www.ibm.com/support/pages/node/7272521

Affected Product	**HP**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-35979, CVE-2025-35991, CVE-2026-20772)
Description	HP has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-35979:** Exposure of sensitive information caused by shared microarchitectural predictor state that influences transient execution for some Intel(R) Processors within VMX non-root (guest) operation may allow an information disclosure. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable data exposure. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. **CVE-2025-35991:** Improper initialization in the UEFI firmware for some Intel platforms within Ring 0: Bare Metal OS may allow an information disclosure. System software adversary with a privileged user combined with a high complexity attack may enable data exposure. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. **CVE-2026-20772:** Uncontrolled search path for some Intel(R) Connectivity Performance Suite software installers. User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. HP advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hp.com/us-en/document/ish_14918841-14918863-16/hpsbhf04115 https://support.hp.com/us-en/document/ish_14915114-14915136-16/hpsbhf04113 https://support.hp.com/us-en/document/ish_14918747-14918774-16/hpsbhf04114

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.