Advisory Alert

Alert Number: AAA20260909 **Date:** September 9, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Commvault	**Critical**	Authentication Bypass Vulnerability
Ivanti	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
SAP	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Lenovo	**High**	Multiple Vulnerabilities
Ivanti	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Cisco	**High**	Secure Boot Bypass Vulnerability
WatchGuard	**High**	Cross-Site Request Forgery (CSRF) Vulnerability
Commvault	**High**, **Medium**	Multiple Vulnerabilities
HPE	**High**, **Medium**	Multiple Vulnerabilities
SAP	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Fortinet	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Citrix	**Medium**	Out of Bounds Read Vulnerability
NETGEAR	**Low**	Multiple Vulnerabilities

Description

Vendor	**Commvault**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2026-77089)
Description	Commvault has released a security update addressing a vulnerability that exists in their products. **CVE-2026-77089:** Command Center API contained an authentication bypass issue affecting privilege management. Software customers upgrade to resolved maintenance release. Commvault advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Commvault (Linux, Windows): • 11.36.0 – 11.36.122 • 11.40.0 – 11.40.71 • 11.44.0 – 11.44.19 • 11.46.0 – 11.46.19
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://documentation.commvault.com/securityadvisories/CV_2026_07_1.html

Vendor	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-12744, CVE-2026-12745, CVE-2026-12650, CVE-2026-12645, CVE-2026-12646, CVE-2026-12647)
Description	Ivanti has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Ivanti advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ivanti Neurons for ITSM: • Cloud / SaaS: 2026.2 • On-Prem: 2025.2, 2025.3, 2025.4, 2026.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Neurons-for-ITSM-Multiple-CVEs?language=en_US

Vendor	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Microsoft has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Microsoft advises to apply these security fixes at your earliest to protect your systems from potential threats.

Affected Products		
	Windows ALPC	RPC Runtime
	Windows Print Spooler Components	Windows Bluetooth Port Driver
	Microsoft Office Excel	Windows Accounts Control
	Windows Kernel	Windows Credential Providers
	Microsoft Authentication Library (MSAL) for Node.js	Active Directory Domain Services
	Windows Key Distribution Center	Windows PowerShell
	Microsoft Graphics Component	Windows TCP/IP
	Windows Resilient File System (ReFS)	Windows Text Shaping
	Deduplication Service	Windows Smart Card
	Remote Desktop Client	Windows DHCP Client
	Windows Message Queuing	Microsoft Office Access
	Windows Error Reporting	Windows DWM Core Library
	Windows NTFS	Windows Network File System
	Windows Imaging Component	Windows Container Manager Service
	Windows Cloud Files Mini Filter Driver	Windows HTTP Print Provider
	Windows Services for NFS ONCRPC XDR Driver	Windows RNDIS
	Windows Biometric Service	Windows Universal Disk Format File System Driver (UDFS)
	Windows Resilient File System (ReFS)	Windows Broadcast DVR User Service
	Microsoft Office Word	Windows Link Layer Topology Discovery Protocol
	Microsoft Azure CLI	HID class driver
	Entra ID	Windows Group Policy
	Windows Device Association Service	Windows Direct Show
	Windows Secure Kernel Mode	Windows Secure Boot
	Microsoft Azure Active Directory B2C	Windows Web Platform Storage
	Windows Virtualization-Based Security (VBS) Enclave	Windows IP Address Management (IPAM) Service
	Windows Update Stack	Windows Device Association Broker service
	Microsoft Office Publisher	Windows Host Guardian Service
	Visual Studio Code	Windows Raw Image Extension
	GitHub Copilot and Visual Studio Code	Windows Notification
	Virtual Hard Disk (VHD) Miniport Driver	Skype for Business
	Windows Hello	Microsoft Exchange Server
	Microsoft Windows Codecs Library	Windows Remote Desktop Licensing Service
	Azure HDInsights	Windows Connected User Experiences and Telemetry
	Copilot Studio	Windows exFAT File System
	Microsoft Authenticator	Windows Image Acquisition
	Windows Remote Desktop Services	Microsoft Install Service
	Microsoft Office	Windows PrintWorkflowUserSvc
	Microsoft Office PowerPoint	Microsoft Windows Media Foundation
	Microsoft Office Outlook	Windows HTTP.sys
	Windows Hyper-V	Microsoft Local Security Authority Server (lsasrv)
	Windows Work Folders	Microsoft Windows PDF
	Windows DNS	Windows Storage Spaces Controller
	Windows Storage	Windows Online Certificate Status Protocol (OCSP)
	Windows CD-ROM Driver	Windows Program Compatibility Assistant Service
	Windows MIDI Service Module	Microsoft Teams for Android
	Windows Security Health Service	Microsoft Partner Center
	SQL Server	Azure Arc
	Microsoft Windows SCSI Class System File	Windows App for Mac
	Reliable Multicast Transport Driver (RMCAST)	Azure Virtual Machines
	Windows Distributed File System (DFS)	Windows Camera Frame Server Monitor
	Windows Failover Cluster	Microsoft Windows Speech
	Windows OLE DB	Windows USB Mass Storage Class Driver
	Azure CycleCloud	Azure Stack HCI
	Microsoft Dynamics 365	Windows Remote Desktop
	Visual Studio	Windows Wireless Networking
	Windows Management Instrumentation	Connected Devices Platform Service (Cdpsvc)
	Windows Volume Manager Extension Driver	Azure SQL Database
	Windows Security Center	Windows Event Logging Service
	Power Automate	Windows Microsoft DirectMusic
	Windows DHCP Server	Windows Overlay Filter
	Windows Installer	Windows Devices Human Interface
	Windows Boot Manager	Windows Power Dependency Coordinator
	Role: DNS Server	Windows BitLocker
	Storage Port Driver	.NET and Visual Studio
	Windows GDI	Microsoft JScript
	Windows iSCSI	Volume Manager Driver
	Windows Modern Device Management (MDM)	Telnet Client
	Windows URL Moniker	Windows Embedded Mode Service
	Graphic Fonts	Windows LDAP - Lightweight Directory Access Protocol
	Windows Graphics Kernel	Windows VOLSNAP.SYS
	Data Sharing Service Client	Windows Kernel Mode Driver
	Windows Management Services	Azure Data Manager for Energy
	Windows Secure Socket Tunneling Protocol (SSTP)	
	Windows Authentication Methods	
	Windows Autopilot	
	Windows USB Hub Driver	

	Windows Volume Shadow Copy Microsoft Edge (Chromium-based) Windows Internet Connection Sharing (ICS) Windows Netlogon IP Helper Active Directory Federation Services (AD FS) Windows Network Connection Broker Windows Remote Access Connection Manager Windows WebClient Service Windows Modern Execution Server Windows USB Video Driver Windows Media Player Windows Routing and Remote Access Service (RRAS) Windows Credential Guard Windows Deployment Services Windows USB Driver Windows Spaceport.sys Windows SMB Server Network Transport Driver (srvnet.sys) Windows File History Service Windows Task Scheduler Role: Windows Fax Service Windows Schannel Windows SMB Client Microsoft WDAC OLE DB provider for SQL Windows Message Queuing Queue Manager Winsock Windows Partition Management Driver Windows Storage Management Provider Windows Work Folder Service Windows NFS Portmapper Windows Device Health Attestation (DHA) Windows Remote Desktop Protocol Windows Paint Windows Core Messaging Windows Mobile Broadband Windows Defender Firewall Service Windows Display Enhancement Service Windows AF_UNIX Socket Provider Windows Shell Windows Audio Service .NET Azure AI Language Microsoft WebP Image Extension Windows Ancillary Function Driver for WinSock Microsoft PowerShell Microsoft PowerShell Core Microsoft Edge for iOS Windows Win32 Kernel Subsystem Windows Win32K Microsoft Fabric Microsoft Windows Search Component Windows Compressed Folder Windows Enterprise App Management Microsoft Office SharePoint Kernel Streaming WOW Thunk Service Driver Windows Media Windows Virtual Trusted Platform Module Windows Bluetooth Service Windows IKE Extension Windows Wireless Wide Area Network Service Windows USB Audio Class driver (usbaudio.sys) Azure Cosmos DB Microsoft Copilot in Azure Spring Cloud Azure Azure Active Directory Windows Encrypting File System (EFS) Windows iSCSI Target Service Microsoft Entra ID Microsoft Standard XPS Windows Kerberos Active Directory Certificate Services (AD CS)	Microsoft Defender Windows SMB Server Audio Video Control Transport Protocol Azure Logic Apps OpenSSH for Windows Windows NDIS Windows Broker Infrastructure Service Windows Storage Port Driver Windows Universal Plug and Play (UPnP) Device Host Windows Fast FAT Driver Remote Desktop Gateway Service Windows Registry BranchCache Windows Performance Monitor Windows License Manager ASP.NET Core Push Message Routing Service Windows Push Notifications Microsoft COM for Windows Windows Setup Files Cleanup Windows GDI+ Windows DCOM Server Microsoft UxTheme Library (uxtheme.dll) Internet Storage Name Service Microsoft Account Windows Bind Filter Driver Windows Package Manager Windows Cross Device Service Azure Data Factory Power BI Microsoft Exchange Online Desktop Window Manager Azure Managed Instance for Apache Cassandra Microsoft Teams Mobile Visual Studio Code CoPilot Chat Extension Windows Remote Access API Microsoft Discovery Studio Microsoft QUIC .NET Framework Windows Common Log File System Driver Windows Brokering File System User-Mode Power Service (UMPS) Winlogon Microsoft High Performance Computing (HPC) Pack AMD Zen Windows Admin Center Copilot Chat (Microsoft Edge) Universal Plug and Play (upnp.dll) Azure Storage Explorer Windows RDP Client Microsoft Fabric Data Warehouse Microsoft Trace Data Helper Windows Server Network driver Windows Server Windows VHD miniport driver Windows Remote Help Windows Remote Help Defense Visual Studio Code - Python extension Windows Internet Key Exchange (IKE) Protocol Microsoft Windows Windows RDP Windows Audio Compression Manager (ACM) Windows OLE Windows Clipboard Server Azure Connected Machine Agent UI Automation Manager (uiamanager.dll) Windows SDK Windows Internet (wininet.dll) Windows RPC API Windows Telephony Service Windows Server Update Service Microsoft Copilot Servicing Stack Updates
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/	

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-62718, CVE-2025-47273, CVE-2026-59890, CVE-2026-48526, CVE-2026-48522, CVE-2026-55200, CVE-2026-43503, CVE-2026-46331, CVE-2026-43499, CVE-2026-46242, CVE-2026-53362, CVE-2025-66418, CVE-2025-66471, CVE-2026-21441, CVE-2026-44431, CVE-2026-25645, CVE-2026-69247, CVE-2026-69249, CVE-2026-39892)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell SmartFabric Manager Versions prior to 2.3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000506597/dsa-2026-406-security-update-for-dell-smartfabric-manager-multiple-third-party-component-vulnerabilities

Vendor	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-66768, CVE-2026-76969, CVE-2026-58240, CVE-2026-44756)
Description	SAP has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. SAP advises to apply these security fixes at your earliest to protect your systems from potential threats.

Affected Products	SAP Platform & Developer Solutions:
	• SAP Cloud Application Programming Model (CAP): Library `@sap/cds-mtxs`
	• SAP Extended Passport (EPP) Processing
	• SAP NetWeaver Infrastructure & Components:
	  ○ Message Server
	  ○ SAP GUI for Java

Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/september-2026.html?isu_page=1

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38403, CVE-2026-43114, CVE-2026-45998, CVE-2026-46056, CVE-2026-46099, CVE-2026-46117, CVE-2026-46145, CVE-2026-53006, CVE-2026-53009, CVE-2026-53196, CVE-2026-63886, CVE-2026-64304, CVE-2026-17523, CVE-2026-53071, CVE-2026-64191, CVE-2021-47600, CVE-2023-52924, CVE-2026-31411, CVE-2026-46120, CVE-2026-53016, CVE-2026-64268, CVE-2026-33814, CVE-2026-42504, CVE-2026-12413, CVE-2026-14164, CVE-2026-14957, CVE-2026-15816, CVE-2026-16313, CVE-2026-50721, CVE-2026-50722)
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 the affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Red Hat Enterprise Linux 8.6 (Advanced Update Support, Extended Life Cycle Long Life): x86_64 • Red Hat Enterprise Linux 9.4 (Advanced Update Support, Update Services for SAP Solutions, Four Years of Updates, Extended Life Cycle): x86_64, aarch64, ppc64le, s390x • Red Hat OpenShift Container Platform 4.20 (RHEL 8 / RHEL 9): x86_64, aarch64, ppc64le, s390x • Red Hat OpenShift Container Platform 4.21 (RHEL 8 / RHEL 9): x86_64, aarch64, ppc64le, s390x • Red Hat OpenShift Container Platform 4.22 (RHEL 8 / RHEL 9): x86_64, aarch64, ppc64le, s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:65712 https://access.redhat.com/errata/RHSA-2026:65711 https://access.redhat.com/errata/RHSA-2026:65710 https://access.redhat.com/errata/RHSA-2026:63091 https://access.redhat.com/errata/RHSA-2026:63041 https://access.redhat.com/errata/RHSA-2026:63093 https://access.redhat.com/errata/RHSA-2026:63100

Vendor	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-8810, CVE-2026-24225, CVE-2026-24262, CVE-2026-24263, CVE-2026-33197, CVE-2026-47624, CVE-2026-47626)
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 the affected systems. Lenovo 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.lenovo.com/us/en/product_security/LEN-226395

Vendor	**Ivanti**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-12648, CVE-2026-12651, CVE-2026-83527, CVE-2026-18851)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Ivanti advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ivanti Enterprise Solutions: • Endpoint Manager Mobile (EPMM): 12.8.0.3 & prior, 12.9.0.1 & prior • Neurons for ITSM (Cloud / SaaS): 2026.2 • Neurons for ITSM (On-Prem): 2025.2, 2025.3, 2025.4, 2026.1 • Sentry: R10.6.3 & prior, R10.7.2 & prior, R10.8.1 & prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://hub.ivanti.com/s/article/Security-Advisory---Ivanti-Endpoint-Manager-Mobile-CVE-2026-18851?language=en_US • https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Neurons-for-ITSM-Multiple-CVEs?language=en_US • https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Sentry-CVE-2026-83527?language=en_US

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-24073, CVE-2026-24074, CVE-2026-66269, CVE-2026-80355, CVE-2026-80356, CVE-2026-81438, CVE-2026-81439, CVE-2026-81440, CVE-2026-81441, CVE-2026-81442, CVE-2026-81443, CVE-2026-81445, CVE-2026-81446, CVE-2026-81447, CVE-2026-81453, CVE-2026-81474, CVE-2026-81475, CVE-2026-81476, CVE-2026-81477, CVE-2026-81478, CVE-2026-81479, CVE-2026-81480, CVE-2026-81481)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.

Affected Products	Dell products utilizing the following software/firmware versions:
	• Qualcomm Adreno Graphics Driver:
	  ○ X1-45 / X1-85 Series: Prior to 31.0.148.0
	• Dell OpenManage Server Administrator (OMSA) Managed Node:
	  ○ Supported OS Platforms (Windows, RHEL 8.10, RHEL 9.4, SLES 15, Ubuntu 22.04): Prior to 11.1.0.3

Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000506556/dsa-2026-145-security-update-for-dell-client-platforms-for-qualcomm-adreno-gpu-display-driver-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000506586/dsa-2026-403-security-update-for-dell-openmanage-server-administrator-omsa-network-access-vulnerabilitiesv

Vendor	**Cisco**
Severity	**High**
Affected Vulnerability	Secure Boot Bypass Vulnerability (CVE-2026-20293)
Description	Cisco has released a security update addressing a vulnerability that exists in their products. **CVE-2026-20293:** A vulnerability in the Unified Extensible Firmware Interface (UEFI) Shell implementation of Cisco UCS Servers and UCS-based appliances could allow an authenticated attacker with valid credentials for a user account with the role of user or admin or an unauthenticated attacker with physical access to an affected device to bypass UEFI Secure Boot validation checks and execute unauthorized software. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.

Affected Products	Cisco Unified Computing System (UCS) & Security Appliances (UEFI Secure Boot Enabled):
	• 5000 Series Enterprise Network Compute Systems (ENCS): CSCwu42927
	• UCS B-Series / C-Series / S-Series / X-Series / Unified Edge: CSCwt77804
	• UCS C845A M8 Rack Server: CSCwt77950
	• UCS C880A M8 Rack Server: CSCwt78022
	• UCS C885A M8 Rack Server: CSCwt77952
	• UCS E-Series M3 Servers: CSCwu42927
	• UCS E-Series M6 Servers: CSCwu42928
	• UCS C-Series Preconfigured Appliances (KVM / Virtual KVM Access Exposed):
	  ○ Application Policy Infrastructure Controller (APIC)
	  ○ Cisco Telemetry Broker
	  ○ HyperFlex Nodes & HyperFlex Edge Nodes
	  ○ IEC6400 Edge Compute
	  ○ IOS XRv 9000 M7
	  ○ Nexus Dashboard
	  ○ Secure Email Gateways
	  ○ Secure Email and Web Manager
	  ○ Secure Endpoint Private Cloud
	  ○ Secure Firewall Management Center (FMC)
	  ○ Secure Malware Analytics
	  ○ Secure Network Analytics
	  ○ Secure Network Server (ISE SNS)
	  ○ Secure Web Appliances

Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-uefi-sb-bypass-eb6xC5GW

Vendor	**WatchGuard**
Severity	**High**
Affected Vulnerability	Cross-Site Request Forgery (CSRF) Vulnerability (CVE-2026-86135)
Description	WatchGuard has released a security update addressing a vulnerability that exists in their products. **CVE-2026-86135:** A Cross-Site Request Forgery (CSRF) vulnerability in WatchGuard Dimension's database snapshot creation feature allows a remote attacker to trigger unauthorized snapshot creation by tricking an authenticated administrator into visiting a specially crafted web page. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WatchGuard Dimension versions 2.0.0 – 2.3.0 (Prior to 2.3.1)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.watchguard.com/CVE-2026-86135/

Vendor	**Commvault**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-77106, CVE-2026-77105, CVE-2026-77104, CVE-2026-77103, CVE-2026-77102, CVE-2026-77101, CVE-2026-77098, CVE-2026-77097, CVE-2026-77092, CVE-2026-77091)
Description	Commvault has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Commvault advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Commvault (Linux, Windows): • 11.36.0 – 11.36.122 • 11.40.0 – 11.40.71 • 11.44.0 – 11.44.19 • 11.46.0 – 11.46.19
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://documentation.commvault.com/securityadvisories/CV_2026_08_8.html • https://documentation.commvault.com/securityadvisories/CV_2026_08_7.html • https://documentation.commvault.com/securityadvisories/CV_2026_08_6.html • https://documentation.commvault.com/securityadvisories/CV_2026_08_5.html • https://documentation.commvault.com/securityadvisories/CV_2026_08_4.html • https://documentation.commvault.com/securityadvisories/CV_2026_08_3.html • https://documentation.commvault.com/securityadvisories/CV_2026_08_2.html • https://documentation.commvault.com/securityadvisories/CV_2026_08_1.html • https://documentation.commvault.com/securityadvisories/CV_2026_07_7.html • https://documentation.commvault.com/securityadvisories/CV_2026_07_6.html • https://documentation.commvault.com/securityadvisories/CV_2026_07_3.html • https://documentation.commvault.com/securityadvisories/CV_2026_07_7.html

Vendor	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20715, CVE-2026-20734, CVE-2026-20708)
Description	HPE has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-20715:** Improper input validation in some firmware for some Intel(R) Active Management Technology (Intel(R) AMT) and some Intel(R) Standard Manageability may allow a denial of service. Network adversary with an unauthenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via network access when attack requirements are present without special internal knowledge and requires no user interaction. **CVE-2026-20734:** Improper initialization in some firmware for some Intel(R) Active Management Technology (Intel(R) AMT), and some Intel(R) Standard Manageability may allow an information disclosure. System software adversary with a privileged user combined with a low 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-2026-20708:** Insertion of sensitive information into log file in the subsystem for the Intel(R) AMT and Intel(R) Standard Manageability may allow an information disclosure. Network adversary with a privileged user combined with a high complexity attack may enable data exposure. This result may potentially occur via network access when attack requirements are not present without special internal knowledge and requires no user interaction. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Infrastructure – Minimum Required BIOS Versions: • HPE Alletra (4110, 4120, 4140): Prior to v3.00_08-20-2026 • HPE Compute Edge Server e930t: Prior to v3.00_08-20-2026 • HPE ProLiant Gen11 (DL110, DL320, DL360, DL380, DL380a, DL560, ML110, ML350): Prior to v3.00_08-20-2026 • HPE ProLiant Gen10 Plus (DL20, ML30, MicroServer v2): Prior to v2.70_08-20-2026 • HPE Synergy 480 Gen11 Compute Module: Prior to v3.00_08-20-2026
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05102en_us&docLocale=en_US

Vendor	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-58234, CVE-2026-76963, CVE-2026-76962, CVE-2026-76959, CVE-2026-76961, CVE-2026-76960, CVE-2026-76977, CVE-2026-34477, CVE-2026-76971, CVE-2026-44766, CVE-2026-76968, CVE-2026-2332, CVE-2026-66767, CVE-2026-76967, CVE-2026-76958, CVE-2026-58243)
Description	SAP has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. SAP advises to apply these security fixes at your earliest to protect your systems from potential threats.

Affected Products	SAP Solutions & Enterprise Applications:
	• SAP ABAP Developer Tools
	• SAP Commerce Cloud (Search and Navigation)
	• SAP Integration Suite
	• SAP Manufacturing Integration and Intelligence (MII)
	• SAP NetWeaver & ABAP Platform:
	  ○ Application Server for ABAP
	  ○ NetWeaver Business Client
	  ○ Process Integration (SOAP Adapter)
	• SAP S/4HANA Module Components:
	  ○ Finance for Advanced Payment Management
	  ○ Intercompany Matching and Reconciliation
	  ○ Manage Bank Chains App
	• SAP Systems Infrastructure & UI Components:
	  ○ SAP Web Dispatcher, Internet Communication Manager (ICM) & SAP Content Server
	  ○ SAPUI5 (Frame Options Allowlist)

Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/september-2026.html?isu_page=1

Vendor	**Fortinet**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-84386, CVE-2026-84387, CVE-2026-84392, CVE-2026-84389, CVE-2026-26084, CVE-2026-84391, CVE-2026-22575, CVE-2026-84393)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Fortinet advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Fortinet Security Fabric Infrastructure: • FortiAnalyzer: 7.6 (7.6.3 – 7.6.6) • FortiClient (Windows): 7.2 (all versions), 7.4 (7.4.0 – 7.4.7) • FortiManager: 7.2 (all versions), 7.4 (7.4.0 – 7.4.10), 7.6 (7.6.0 – 7.6.4) • FortiManager Cloud: 7.2 (all versions), 7.4 (7.4.1 – 7.4.10), 7.6 (7.6.2 – 7.6.4) • FortiOS: 7.2 (all versions), 7.4 (all versions), 7.6 (7.6.1 – 7.6.6) • FortiPAM: 1.0 – 1.8 (all versions), 1.9 (1.9.0) • FortiProxy: 7.2 (all versions), 7.4 (all versions), 7.6 (7.6.0 – 7.6.6) • FortiSandbox: 4.4 (4.4.0 – 4.4.9), 5.0 (5.0.0 – 5.0.6), 5.2 (5.2.0) • FortiSandbox Cloud / PaaS: 5.0 (5.0.4 – 5.0.5) • FortiSIEM: 7.4 (7.4.1 – 7.4.2), 7.5 (7.5.0 – 7.5.1)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-26-165 https://www.fortiguard.com/psirt/FG-IR-26-167 https://www.fortiguard.com/psirt/FG-IR-26-173 https://www.fortiguard.com/psirt/FG-IR-26-169 https://www.fortiguard.com/psirt/FG-IR-26-166 https://www.fortiguard.com/psirt/FG-IR-26-172 https://www.fortiguard.com/psirt/FG-IR-26-171 https://www.fortiguard.com/psirt/FG-IR-26-174

Vendor	**Citrix**
Severity	**Medium**
Affected Vulnerability	Out of Bounds Read Vulnerability (CVE-2026-78546, CVE-2026-78547)
Description	Citrix has released a security update addressing a vulnerability that exists in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Citrix advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Citrix Workspace app for Windows: • Current Release (CR): Prior to 2603.11 • Long Term Service Release (LTSR): Prior to 2507.1 LTSR CU3, Prior to 2607 LTSR
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697034&articleURL=Citrix_Workspace_app_for_Windows_Security_Bulletin_CVE_2026_78546_and_CVE_2026_78547

Vendor	**NETGEAR**
Severity	**Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-9215, CVE-2026-9216)
Description	NETGEAR has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-9215:** A cross site request forgery (CSRF) vulnerability in the listed NETGEAR models allows an attacker, who can leverage social engineering techniques on a router administrator, to tamper with router configuration and disrupt router operations with active assistance from the router administrator. **CVE-2026-9216:** The vulnerability allows a network-adjacent attacker with network access (such as WiFi credentials) to crash affected router's management UI. There is no confidentiality or integrity impact. A crash of the router's management UI does not impact the availability of the router's core services like its WiFi network. NETGEAR advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NETGEAR Nighthawk Routers: • RAX30: BIOS/Firmware prior to v1.0.9.92 • RAX35, RAXE300: BIOS/Firmware prior to v1.0.10.72 • RAX38 (EoS), RAX40 (EoS): BIOS/Firmware prior to v1.0.6.106 • XR500 (EoS): BIOS/Firmware prior to v2.3.5.152 • XR1000, XR1000v2: BIOS/Firmware prior to v1.1.0.22
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.netgear.com/000070912/September-2026-NETGEAR-Security-Advisory

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.