Advisory Alert

Alert Number: AAA20261014 **Date:** October 14, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
Commvault	**Critical**	Input Validation Vulnerability
Ivanti	**Critical**	Multiple Vulnerabilities
HPE	**Critical**	Security Update
Fortinet	**Critical**	Security Update
IBM	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
SAP	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
HPE	**High**, Low	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Commvault	**High**, Medium	Multiple Vulnerabilities
Citrix	**High**, Medium	Multiple Vulnerabilities
Ivanti	**High**, Medium	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
MongoDB	**High**, Medium	Multiple Vulnerabilities
Fortinet	**High**, Medium, Low	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
Ubuntu	**High**, Medium, Low	Multiple Vulnerabilities
SAP	**High**, Medium, Low	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Red Hat 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. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat AI Inference Server
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:82368

Vendor	**Commvault**
Severity	**Critical**
Affected Vulnerability	Input Validation Vulnerability (CVE-2026-77099)
Description	Commvault has released a security update addressing a vulnerability that exists in their products. **CVE-2026-77099:** CVFS contained an input validation issue affecting command execution. Software customers upgrade to resolved maintenance release. Update CVFS. Commvault advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Commvault Infrastructure: Commvault Linux: • 11.36.0 – 11.36.126 • 11.40.0 – 11.40.77 • 11.44.0 – 11.44.24 • 11.46.0 – 11.46.29 Grid(HSX) CVFS Linux: 5.0.1.0 – 5.0.14.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://documentation.commvault.com/securityadvisories/CV_2026_10_9.html

Vendor	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-106042, CVE-2026-109412)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-106042:** An External Control of File Name or Path vulnerability in Ivanti Xtraction before version 2026.4 allows a remote authenticated attacker to redirect application-generated requests to an attacker-controlled endpoint and obtain EPMM connector credentials transmitted by the application. **CVE-2026-109412:** An exposed dangerous endpoint in Ivanti Neurons Patch for Intune allows a remote authenticated attacker to leak sensitive authentication information. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Neurons Patch for Intune Ivanti Xtraction versions 2026.2.1 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Xtraction-Multiple-CVEs?language=en_US https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Neurons-Patch-for-Intune-October-2026?language=en_US

Vendor	**HPE**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2026-65206)
Description	HPE has released a security update addressing a vulnerability that exists in their products. **CVE-2026-65206:** Potential security vulnerabilities have been identified in HPE Integrated Lights-Out 5 (iLO 5), Integrated Lights-Out 6 (iLO 6), and Integrated Lights-Out 7 (iLO 7). These vulnerability could be remotely exploited to allow denial of service and authentication bypass. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Servers - prior to 3.22 HPE Integrated Lights-Out 6 (iLO 6) - prior to 1.79 HPE Integrated Lights-Out 7 (iLO 7) - prior to 1.25.01
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05170en_us&docLocale=en_US

Vendor	**Fortinet**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2026-106173, CVE-2026-107656)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-106173:** A improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiSIEM 7.5.0 may allow attacker to execute unauthorized code or commands via specially crafted packets. **CVE-2026-107656:** An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] in FortiSandbox GUI may allow a remote unauthenticated attacker to bypass authentication via crafted HTTP requests. Fortinet advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Fortinet Infrastructure: FortiSIEM: 7.5.0 FortiSandbox: 4.4 (all versions), 4.4.0 – 4.4.9, 5.0.0 – 5.0.6 FortiSandbox PaaS: 5.0.0 – 5.0.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-26-180 https://www.fortiguard.com/psirt/FG-IR-26-185

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Security & Software Products: IBM QRadar: 7.5.0 – 7.5.0 UP16 IF01, 7.6.0.0 – 7.6.0.4 IBM Security Verify Access / Docker: 10.0 – 10.0.9.3 IBM Verify Identity Access / Docker: 11.0 – 11.0.3.1 WebSphere Application Server: 8.5, 9.0 WebSphere Application Server - Liberty: 17.0.0.3 – 26.0.0.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7292236 https://www.ibm.com/support/pages/node/7292219 https://www.ibm.com/support/pages/node/7292228 https://www.ibm.com/support/pages/node/7290794

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	.NET .NET and Visual Studio .NET Framework Active Directory Certificate Services (AD CS) Active Directory Domain Services Active Directory Federation Services (AD FS) ASP.NET Core Audio Video Control Transport Protocol Azure Active Directory Azure AI Foundry Azure API Center Azure App Service Azure Arc Azure Billing Azure Cosmos DB Azure CycleCloud Azure Database for PostgreSQL Azure DevOps Azure Event Grid Azure HDInsight Azure Key Vault Azure Logic Apps Azure Machine Learning Azure Portal Azure SRE Agent Azure Storage Library Connected Devices Platform Service (Cdpsvc) Desktop Window Manager Dynamics Business Central Function Discovery Service (fdwsd.dll) Graphic Fonts HID class driver HID Parser Library Internet Explorer Linux Kernel M365 Copilot Microsoft 365 Copilot's Business Chat Microsoft Account Microsoft Azure Attestation service and Device Health Attestation Service Microsoft Bluetooth Driver Microsoft Bookings Microsoft COM for Windows Microsoft Configuration Manager Microsoft Container Registry Microsoft Copilot Microsoft Dataverse	Windows DWM Core Library Windows EAPHost Service Windows Embedded Mode Service Windows Encrypting File System (EFS) Windows Enterprise App Management Windows Error Reporting Windows Event Logging Service Windows Event Tracing Windows Event Viewer Windows exFAT File System Windows Failover Cluster Windows Fast FAT Driver Windows Fax and Scan Service Windows File History Service Windows GDI Windows GDI+ Windows Geotag Broker Windows Graphics Kernel Windows Group Policy Windows Health and Optimized Experiences Service Windows Hello Windows Host Guardian Service Windows HTTP.sys Windows Hyper-V Windows IKE Extension Windows Image Acquisition Windows Imaging Component Windows Input System Windows Installer Windows Internal System User Profile Windows Internet (wininet.dll) Windows Internet Connection Sharing (ICS) Windows Internet Information Services Windows Internet Key Exchange (IKE) Protocol Windows IP Over USB Service Windows iSCSI Windows iSCSI Target Service Windows Kerberos Windows Kernel Windows Kernel Mode Driver Windows kernel32.dll Windows Kernel-Mode Drivers Windows Key Distribution Center Windows Key Storage Provider Windows Libarchive Windows License Manager Windows Link Layer Topology Discovery

	Microsoft Defender Microsoft Defender for Endpoint Microsoft Digest Authentication Microsoft Edge (Chromium-based) Microsoft Exchange Server Microsoft Fabric Microsoft Failover Cluster Virtual Driver Microsoft Graphics Component Microsoft High Performance Computing (HPC) Pack Microsoft Input Method Editor (IME) Microsoft Install Service Microsoft Internet Messaging API Microsoft Local Security Authority Server (lsasrv) Microsoft MPEG-2 Video Extension Microsoft Office Microsoft Office Access Microsoft Office Click-To-Run Microsoft Office Excel Microsoft Office OneNote Microsoft Office Outlook Microsoft Office PowerPoint Microsoft Office SharePoint Microsoft Office Visio Microsoft Office Word Microsoft Partner Center Microsoft PostScript Printer Driver Microsoft Power Apps Microsoft PowerShell Microsoft PowerToys Microsoft QUIC Microsoft Scripting Engine Microsoft Streaming Service Microsoft Trace Data Helper Microsoft Windows Codecs Library Microsoft Windows Media Foundation Microsoft Windows PDF Microsoft Windows SCSI Class System File Microsoft Windows Search Component Microsoft XML Network Device Enrollment Service (NDES) Network Policy Server (NPS) OpenSSH for Windows Python Quality Windows Audio/Video Experience (QWAVE) service Reliable Multicast Transport Driver (RMCAST) Remote Access Point-to-Point Protocol (PPP) EAP-TLS Remote Desktop Client Remote Desktop Display Driver Remote Desktop Gateway Service Role: DNS Server RPC Endpoint Mapper Service RPC Runtime Servicing Stack Updates Skype for Business and Microsoft Lync Software Protection Platform (SPP) SQL Server SQLite SysInternals Virtual Hard Disk (VHD) Miniport Driver Visual Studio Visual Studio Code Visual Studio Code - Python extension Visual Studio Code CoPilot Chat Extension Visual Studio Tools for Applications and SQL Server Management Studio WebDAV Windows Advanced Rasterization Platform Windows Aggregated Data Platform Service Windows AI Windows ALPC Windows Ancillary Function Driver for WinSock Windows App Installer Windows Application Compatibility Cache Windows AppX Deployment Extensions Windows AppX Deployment Service Windows Assigned Access Windows Audio Service Windows Autopilot Windows Background Intelligent Transfer Service (BITS) Windows Backup Engine	Protocol Windows Local Security Authority (LSA) Windows Local Security Authority Subsystem Service (LSASS) Windows Management Instrumentation Windows Management Services Windows Media Windows Media Player Windows Media Video Decoder Windows Message Queuing Windows Message Queuing Queue Manager Windows MIDI Service Module Windows Mobile Broadband Windows Mobile Device Management Windows Modern Device Management (MDM) Windows NDIS Windows NetBIOS Windows Netlogon Windows Network File System Windows Network List Service Windows Network Load Balancing Windows Notification Windows Now Playing Session Manager Windows NTFS Windows NTLM Windows OLE Windows OLE DB Windows Overlay Filter Windows Paint Windows Partition Management Driver Windows PCI Bus Driver Windows Perception Simulation Service Windows Performance Monitor Windows Phone Service Windows Portable Device Enumerator Service Windows Portable Device File System Driver Windows Portable Device MTP Driver Windows PowerShell Windows Print Spooler Components Windows Program Compatibility Assistant Service Windows Projected File System Windows Push Notifications Windows Quality of Service (QoS) Packet Scheduler Windows Raw Image Extension Windows Registry Windows Remote Access Connection Manager Windows Remote Access Service Infrastructure Windows Remote Desktop Windows Remote Desktop Protocol Windows Remote Desktop Services Windows Remote POS Driver Windows Resilient File System (ReFS) Windows Resilient File System (ReFS) Deduplication Service Windows Resource Management (MRM) Windows Resume Windows Rich Text Edit Control Windows RNDIS Windows Routing and Remote Access Service (RRAS) Windows Schannel Windows Secure Boot Windows Secure Kernel Mode Windows Secure Socket Tunneling Protocol (SSTP) Windows Security Account Manager Windows Security App Windows Security Center Windows Security Support Provider Interface Windows Sensor Data Service Windows Server Windows Server for NFS Windows Server Update Service Windows Setup and Deployment Windows Setup Files Cleanup Windows Shell Windows Smart Card Windows SmartScreen Windows SMB Client Windows SMB Server Windows Spaceport.sys Windows State Repository Service Windows StateRepository API Windows Storage

	Windows Bind Filter Driver Windows Biometric Service Windows BitLocker Windows Bluetooth A2DP driver Windows Bluetooth Port Driver Windows Bluetooth Service Windows Broadcast DVR User Service Windows Brokering File System Windows Camera Frame Server Monitor Windows Cash Drawer Protocol Provider Windows CCFFilter Driver Windows CD-ROM Driver Windows Certificates Windows Client for NFS Windows Client License Service Windows Client Side Caching driver (csc.sys) Windows Client-Side Caching (CSC) Service Windows Clipboard Server Windows Clipboard User Service Windows Cloud Files Mini Filter Driver Windows COM+ Event System Service Windows Common Log File System Driver Windows Composite Image File System Windows Connected Devices Platform Service Windows Connected User Experiences and Telemetry Windows Console Driver Windows Container Isolation FS Filter Driver Windows Container Isolation FS Filter Driver (unionfs.sys) Windows Core Messaging Windows Credential Guard Windows Credential Manager Windows Credential Providers Windows Cross Device Service Windows Cryptographic Services Windows DCOM Server Windows Defender Firewall Service Windows Deployment Services Windows Device Association Broker service Windows Device Association Service Windows Device Install Service Windows DHCP Client Windows DHCP Server Windows Diagnostic Policy Service Windows Direct Composition Windows DirectX Windows Distributed File System (DFS) Windows DNS	Windows Storage Management Provider Windows Storage Port Driver Windows Storage Spaces Controller Windows Storage VSP Driver Windows Storport Miniport Driver Windows Subsystem for Linux Windows Sysmain Service Windows System Information Console Windows TCP/IP Windows Telephony Server Windows Text Services Framework Windows Text Shaping Windows UEFI Windows UI Immersive Server Windows Universal Disk Format File System Driver (UDFS) Windows Universal Plug and Play (UPnP) Device Host Windows Update Windows Update Delivery Optimization Windows Update Orchestrator Service Windows Update Service Windows Update Stack Windows USB Audio Class driver (usbaudio.sys) Windows USB Driver Windows USB Hub Driver Windows USB Print Driver Windows USB Video Driver Windows User Profile Service Windows VHD miniport driver Windows Virtual Input Windows Virtualization-Based Security (VBS) Enclave Windows VMSwitch Windows Volume Manager Extension Driver Windows WalletService Windows Web Account Manager Windows Web Proxy Auto-Discovery Protocol (WPAD) Windows Wi-Fi Driver Windows Win32 Kernel Subsystem Windows Win32K Windows Win32K - GRFX Windows Win32K - ICOMP Windows Wired AutoConfig Service Windows WLAN Service Windows Work Folders Windows Workstation Service Winlogon
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/vulnerability	

Vendor	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-89111, CVE-2026-89110, CVE-2026-89107, CVE-2026-89108)
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 Systems & Applications: • SAP Cloud SDK for Python versions prior to 0.45.2 • SAP Manufacturing Integration and Intelligence (Configuration Service): XMII 15.4, 15.5 • SAP NetWeaver Visual Composer: VC70RUNTIME 7.50 • SAP S/4HANA (Manage Substitution/Validation Rules): S4CORE 105, 106, 107, 108, 109
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/october-2026.html?isu_page=1

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
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 Platform & Enterprise Software: • Cert Manager support for Red Hat OpenShift release • Red Hat OpenShift Container Platform 4.21 (RHEL 8 / 9): aarch64, ppc64le, s390x, x86_64 • Red Hat OpenShift for Windows Containers
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:82354 https://access.redhat.com/errata/RHSA-2026:82347 https://access.redhat.com/errata/RHSA-2026:82336 https://access.redhat.com/errata/RHSA-2026:79153 https://access.redhat.com/errata/RHSA-2026:82322 https://access.redhat.com/errata/RHSA-2026:82440

Vendor	**HPE**
Severity	**High**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-65204, CVE-2026-65205, CVE-2026-65207, CVE-2026-65208, CVE-2026-65209)
Description	HPE 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. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Servers - prior to 3.22 HPE Integrated Lights-Out 6 (iLO 6) - prior to 1.79 HPE Integrated Lights-Out 7 (iLO 7) - prior to 1.25.01
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05170en_us&docLocale=en_US

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SUSE Infrastructure: SUSE Linux Enterprise 11 SP4: Server (including LTSS Extreme Core) SUSE Linux Enterprise 15 SP7: Live Patching, Real Time (including Real Time Module), Server, Server for SAP Applications
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20264639-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264640-1/

Vendor	**Commvault**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-97334, CVE-2026-97333, CVE-2026-18228, CVE-2026-77100, CVE-2026-77096, CVE-2026-77095, CVE-2026-77094, CVE-2026-77093, CVE-2026-77090)
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 Infrastructure: Commvault Linux: • 11.36.0 – 11.36.126 • 11.40.0 – 11.40.77 • 11.44.0 – 11.44.24 • 11.46.0 – 11.46.39 Commvault Linux, Windows: • 11.36.0 – 11.36.126 • 11.40.0 – 11.40.77 • 11.44.0 – 11.44.24 • 11.46.0 – 11.46.29 Grid(HSX) CVFS Linux: 5.0.1.0 – 5.0.14.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://documentation.commvault.com/securityadvisories/CV_2026_10_3.html https://documentation.commvault.com/securityadvisories/CV_2026_10_4.html https://documentation.commvault.com/securityadvisories/CV_2026_10_8.html https://documentation.commvault.com/securityadvisories/CV_2026_10_6.html https://documentation.commvault.com/securityadvisories/CV_2026_10_10.html https://documentation.commvault.com/securityadvisories/CV_2026_10_7.html https://documentation.commvault.com/securityadvisories/CV_2026_10_5.html https://documentation.commvault.com/securityadvisories/CV_2026_10_1.html https://documentation.commvault.com/securityadvisories/CV_2026_10_2.html https://documentation.commvault.com/securityadvisories/CV_2026_07_4.html

Vendor	**Citrix**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53562, CVE-2026-53563, CVE-2026-53564, CVE-2026-79610, CVE-2026-102700, CVE-2026-102701, CVE-2026-79611, CVE-2026-84419, CVE-2026-84420)
Description	Citrix 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. Citrix advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Citrix Infrastructure: • Citrix UniconOS (Current Release): before 2607.2 • Citrix UniconOS (LTSR): before 2603 LTSR CU2 • XenServer versions 8.4 and 9 • Citrix Workspace app for Windows (Current Release): before 2603.20 • Citrix Workspace app for Windows (LTSR): before 2507 CU3, before 2607
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697187&articleURL=Citrix_UniconOS_Security_Bulletin_CVE_2026_53562_CVE_2026_53563_and_CVE_2026_53564 • https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697170&articleURL=XenServer_Security_Update_for_CVE_2026_79610_CVE_2026_79610_CVE_2026_102700_and_CVE_2026_102701 • https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697181&articleURL=Citrix_Workspace_App_for_Windows_Security_Bulletin_CVE_2026_84419_and_CVE_2026_84420

Vendor	**Ivanti**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-106034, CVE-2026-106035, CVE-2026-106043, CVE-2026-106047, CVE-2026-104935)
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 Infrastructure: Ivanti Xtraction: 2026.2.1 and prior Ivanti Connect Secure (ICS) versions: • 22.8R2.4 and prior • 25.1.1.1 and prior • 25.1.2.2 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Xtraction-Multiple-CVEs?language=en_US https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935?language=en_US

Vendor	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-82150, CVE-2026-82138, CVE-2026-82142, CVE-2026-82139, CVE-2026-82143, CVE-2026-82145, CVE-2026-82136, CVE-2026-82149, CVE-2026-82146, CVE-2026-82140, CVE-2026-86375, CVE-2026-71170, CVE-2026-71169, CVE-2026-82166, CVE-2026-25258, CVE-2026-25260, CVE-2026-25259, CVE-2026-25261)
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 & Qualcomm Infrastructure: Dell Application Installer: prior to 26.09.0.1 Dell Application Store: prior to 26.05.0.7 Dell SupportAssist OS Recovery: prior to 5.5.16.3 Qualcomm MIPI Camera Driver: prior to 1.1.0.61, 1.1.0.63, 1.1.1.17
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000511813/dsa-2026-426-security-update-for-dell-supportassist-os-recovery-for-multiple-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000510641/dsa-2026-423-security-update-for-dell-application-installer-for-a-missing-encryption-of-sensitive-data-vulnerability https://www.dell.com/support/kbdoc/en-us/000506927/dsa-2026-411-security-update-for-dell-application-store-for-multiple-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000509415/dsa-2026-420-security-update-for-dell-client-platform-for-a-qualcomm-mipi-camera-driver-vulnerability

Vendor	**MongoDB**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-104005, CVE-2026-104004, CVE-2026-103965, CVE-2026-96299, CVE-2026-96297)
Description	MongoDB 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. MongoDB advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	MongoDB Server: • 7.0 (affects versions prior to 7.0.45) • 8.0 (affects versions prior to 8.0.34) • 8.3.0 (affects versions prior to 8.3.13) • 9.0 (affects versions prior to 9.0.2, 9.0.4)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.mongodb.com/resources/products/alerts#security

Vendor	**Fortinet**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-106176, CVE-2026-106175, CVE-2026-106172, CVE-2026-106174, CVE-2025-46773, CVE-2026-23705, CVE-2026-23706, CVE-2026-23707, CVE-2026-106170, CVE-2025-57739, CVE-2026-106171)
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 Infrastructure: FortiAnalyzer: 7.2 (all versions), 7.4.0 – 7.4.7, 7.6.0 – 7.6.4 FortiManager: 7.2 (all versions), 7.4.0 – 7.4.6, 7.6.0 – 7.6.6, 8.0.0 FortiMail: 7.2.0 – 7.2.8, 7.4.0 – 7.4.5, 7.6.0 – 7.6.3 FortiProxy: 7.2 (all versions), 7.4 (all versions), 7.6.0 – 7.6.6 FortiSandbox: 4.4 (all versions), 5.0.0 – 5.0.6, 5.2.0 – 5.2.1 FortiSIEM: 7.5 (all versions) FortiOS: 7.2 (all versions), 7.4 (all versions), 7.6.0 – 7.6.7, 8.0.0 FortiSwitch: 7.2 (all versions), 7.4 (all versions), 7.6.0 – 7.6.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-26-183 https://www.fortiguard.com/psirt/FG-IR-26-182 https://www.fortiguard.com/psirt/FG-IR-26-179 https://www.fortiguard.com/psirt/FG-IR-26-181 https://www.fortiguard.com/psirt/FG-IR-26-178 https://www.fortiguard.com/psirt/FG-IR-26-176 https://www.fortiguard.com/psirt/FG-IR-26-184 https://www.fortiguard.com/psirt/FG-IR-26-177

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Security & Software Products: IBM QRadar: 7.5.0 – 7.5.0 UP16 IF01, 7.6.0.0 – 7.6.0.4 IBM QRadar SIEM HTTP Receiver: 7.4-20210823144546 – 7.5-20260930064858, 7.6-20260330053257 – 7.6-20260930064910 IBM Security Verify Access / Docker: 10.0 – 10.0.9.3 IBM Verify Identity Access / Docker: 11.0 – 11.0.3.1 WebSphere Application Server: 8.5, 9.0 WebSphere Application Server - Liberty: 17.0.0.3 – 26.0.0.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7292240 https://www.ibm.com/support/pages/node/7292244 https://www.ibm.com/support/pages/node/7292213 https://www.ibm.com/support/pages/node/7292214 https://www.ibm.com/support/pages/node/7292216 https://www.ibm.com/support/pages/node/7292217 https://www.ibm.com/support/pages/node/7292219 https://www.ibm.com/support/pages/node/7292235 https://www.ibm.com/support/pages/node/7292232 https://www.ibm.com/support/pages/node/7292228 https://www.ibm.com/support/pages/node/7292227 https://www.ibm.com/support/pages/node/7292226 https://www.ibm.com/support/pages/node/7292221 https://www.ibm.com/support/pages/node/7290794

Vendor	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu 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. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu versions 14.04, 16.04, 18.04, 20.04 and 24.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8924-1 https://ubuntu.com/security/notices/USN-8918-1 https://ubuntu.com/security/notices/USN-8921-1 https://ubuntu.com/security/notices/USN-8920-1 https://ubuntu.com/security/notices/USN-8923-1 https://ubuntu.com/security/notices/USN-8919-1 https://ubuntu.com/security/notices/USN-8922-1 https://ubuntu.com/security/notices/USN-8917-1

Vendor	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-89113, CVE-2026-58249, CVE-2026-89120, CVE-2026-89112, CVE-2026-76972, CVE-2026-24316, CVE-2025-42938, CVE-2026-89117, CVE-2026-76975, CVE-2026-89122, CVE-2026-89116, CVE-2026-76976, CVE-2026-89118, CVE-2026-89121, CVE-2026-89106, CVE-2026-89124, CVE-2026-89105, CVE-2026-58242)
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	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/october-2026.html?isu_page=1

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.