Advisory Alert

Alert Number: AAA20260715 **Date:** July 15, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
SonicWall	**Critical**	Multiple Vulnerabilities
SAP	**Critical**	Multiple Vulnerabilities
ASUS	**Critical**	Remote Code Execution Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Lenovo	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Ivanti	**High**, Medium	Multiple Vulnerabilities
ASUS	**High**, Medium	Multiple Vulnerabilities
SAP	**High**, Medium, Low	Multiple Vulnerabilities
Fortinet	**High**, Medium, Low	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
NETGEAR	Medium	Multiple Vulnerabilities
Citrix	Medium	Privilege Escalation Vulnerability

Description

Vendor	**SonicWall**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-15409, CVE-2026-15410)
Description	SonicWall has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-15409:** A Server-side request forgery (SSRF) vulnerability has been identified in the SMA1000 Appliance Work Place interface. A remote unauthenticated attacker could potentially cause the appliance to make requests to unintended location. **CVE-2026-15410:** Post-authentication improper control of generation of code ('Code Injection') vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) which in specific conditions could potentially enable a remote authenticated attacker as administrator to execute arbitrary OS commands. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SMA1000 Models - 6210, 7210, 8200v versions: • 12.4.3-03245, 12.4.3-03387 and 12.4.3-03434 (platform-hotfix) • 12.5.0-02283, 12.5.0-02624 and 12.5.0-02800 (platform-hotfix)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008

Vendor	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-44747, CVE-2026-27690, CVE-2026-44761, CVE-2026-40128)
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 NetWeaver Application Server ABAP versions KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, KERNEL 7.22, 7.53. 7.54, 7.77, 7.89, 7.93, 9.16, 9.18, 9.19, 9.20 • SAP Approuter node.js package prior to 20.10.0 • SAP Commerce Cloud versions HY_COM 2205, COM_CLOUD 2211, 2211-JDK21 • SAP NetWeaver Application Server Java (Web Container) version ENGINEAPI 7.50
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes

Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/july-2026.html

Vendor	**ASUS**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2026-13385)
Description	ASUS has released a security update addressing a vulnerability that exists in their products. **CVE-2026-13385:** An Improper Validation of Integrity Check Value and Improper Certificate Validation in certain ASUS router models allows a remote man-in-the-middle(MITM) user to make the router download and execute arbitrary command via a spoofed server. ASUS advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ASUSWRT firmware 3.0.0.4_386 series, 3.0.0.4_388 series, and 3.0.0.6_102 series: • CN SKU models using the UU feature only
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.asus.com/security-advisory

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-42043, CVE-2026-42044, CVE-2026-42264, CVE-2026-29063, CVE-2026-27459, CVE-2026-4800, CVE-2025-62718)
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	QRadar User Behavior Analytics versions 1.0.0 - 5.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7279973

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
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 PowerProtect Data Manager versions prior to 20.2.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000488847/dsa-2026-287-security-update-dell-power-protect-data-manager-for-multiple-security-vulnerabilities

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	Power BI Microsoft Office SharePoint Windows NTFS Windows Boot Loader Windows Client-Side Caching (CSC) Service Window PC Manager Windows Narrator Braille Desktop Window Manager Windows Win32K Windows Admin Center Windows DirectX Windows Wireless Networking Windows DHCP Server Windows Remote Desktop Services Windows Sensor Data Service	Windows Telephony Service Windows Remote Access Connection Manager Windows BitLocker .NET Azure Active Directory .NET Framework Github Copilot Windows Wireless Wide Area Network Service Windows Message Queuing Windows Event Logging Service Windows Netlogon Windows Universal Disk Format File System Driver (UDFS) Windows Remote Desktop Protocol

	Microsoft Office Excel Microsoft 365 Copilot for iOS Windows Kernel Windows Cloud Files Mini Filter Driver Microsoft Windows Media Foundation Microsoft Graphics Component Windows Print Spooler Components Windows Kernel Mode Driver Virtual Hard Disk (VHD) Miniport Driver Microsoft Edge (Chromium-based) Microsoft Bing App for IOS Windows RDP Universal Plug and Play (upnp.dll) Windows Management Services Windows USB Print Driver Windows Media Windows DWM Windows Installer Windows Bluetooth Service Microsoft NAT Helper Components (ipnathlp.dll) Microsoft Input Method Editor (IME) Windows SMB Windows Resilient File System (ReFS) Active Directory Federation Services (AD FS) Windows USB Audio Class driver (usbaudio.sys) Windows Runtime Windows Storage Microsoft Edge for Android Azure CycleCloud Active Directory Domain Services Windows Subsystem for Linux .NET Core Visual Studio Code Microsoft XML Windows Routing and Remote Access Service (RRAS) Windows Ancillary Function Driver for WinSock Windows VMSwitch Windows File History Service Windows SMB Server Network Transport Driver (srvnet.sys) Extensible Storage Engine (ESENT) Windows File Explorer Microsoft Windows Codecs Library Windows Network File System Windows Remote Access Service Infrastructure Microsoft Fabric Data Warehouse Microsoft Office Windows Server Network driver Windows MIDI Service Module Windows Schannel Windows Network Address Translation (NAT) Microsoft Defender for Endpoint Windows Win32K - GRFX Windows WebView ASP.NET Core Windows SMB Server Microsoft Dynamics NAV Outlook Copilot Windows CryptoAPI Microsoft Office Word Microsoft Office OneNote Microsoft Office PowerPoint Windows Remote Help Defense Microsoft Defender Microsoft Exchange Server Microsoft Printer Drivers SQL Server Windows Active Directory Windows TCP/IP Reliable Multicast Transport Driver (RMCAST) Windows Message Queuing Queue Manager Remote Desktop Client Quality Windows Audio/Video Experience (QWAVE) service Windows Overlay Filter Windows Hyper-V Windows DHCP Client Windows Terminal Windows GDI+ Active Directory Certificate Services (AD CS) Windows Common Log File System Driver Windows Internet Key Exchange (IKE) Protocol Windows Secure Socket Tunneling Protocol (SSTP) Windows Clipboard Server Windows OLE Windows Cryptographic Services Microsoft Windows Search Component	Windows Network Policy Server SNMP Windows DNS Windows Graphics Kernel Code Integrity DLL (ci.dll) Windows Clipboard User Service Windows Web Proxy Auto-Discovery Protocol (WPAD) Windows USB Hub Driver Microsoft Windows Windows Projected File System Windows Brokering File System Windows User Interface Core Windows Server Update Service Windows Audio Service Windows DWM Core Library Windows Push Notifications Windows Virtual Filtering Platform (VFP) Windows Quality of Service (QoS) Packet Scheduler Windows Container Isolation FS Filter Driver (unionfs.sys) Content Delivery Manager Role: DNS Server Windows Internal System User Profile Windows Domain Controller Windows Connected User Experiences and Telemetry Windows HTTP.sys Windows System Windows Backup Engine Windows Filtering Platform (WFP) Windows App Installer Windows Kernel-Mode Drivers Windows Secure Kernel Mode Windows Group Policy Windows GDI Windows Clip Service Composite Image File System Driver Windows Key Guard Windows Redirected Drive Buffering Windows LUAFV Windows RPC API Windows Server Backup Microsoft XML Core Services Microsoft Windows App Store Windows Audio Compression Manager (ACM) Windows Trusted Runtime Interface Driver Windows Data.dll RPC Runtime Microsoft Install Service Azure Spring Apps Windows Notification Windows Operating Systems Windows Spaceport.sys Windows Application Model Windows Unified Consent System Windows USB Driver Windows Image Acquisition Windows Server Windows Devices Human Interface Windows Storage Spaces Direct Windows Internal Task Bar Windows USB Video Driver Windows AppX Deployment Service Windows Local Security Authority Subsystem Service (LSASS) HTTP/2 Windows Secure Boot Windows WalletService Windows FTP Service Microsoft Windows Speech Windows StateRepository API Microsoft Surface Microsoft Copilot Azure Monitor Agent Visual Studio Microsoft Configuration Manager GitHub Copilot and Visual Studio Code Office for Android SQL Server ODBC driver Windows NT OS Kernel Windows Bluetooth Port Driver Windows Hotpatch Monitoring Service Windows Kerberos Windows Projected File System Filter Driver GitHub Copilot and Visual Studio Windows PowerShell Microsoft Dynamics 365 (on-premises) Windows Win32K - ICOMP Servicing Stack Updates
Officially Acknowledged by the Vendor	Yes	

Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53016, CVE-2025-38653, CVE-2025-68183, CVE-2025-68724, CVE-2026-31408, CVE-2026-43027, CVE-2026-43074, CVE-2026-43330, CVE-2026-43414, CVE-2026-46116, CVE-2026-46173, CVE-2026-46135, CVE-2026-46242, CVE-2026-46316, CVE-2026-53359, CVE-2026-34486, CVE-2026-29146, CVE-2026-43515, CVE-2026-41284, CVE-2026-41293, CVE-2026-42498, CVE-2026-43512, CVE-2026-43513, CVE-2026-43514, CVE-2026-55956, CVE-2026-2673, CVE-2025-71066, CVE-2025-71089, CVE-2026-31411, CVE-2026-43499, CVE-2026-46113, CVE-2026-53266, CVE-2026-53166)
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 10 Red Hat Enterprise Linux - Extended Update Support 10.2 Red Hat Enterprise Linux - Extended Update Support 10.0 Red Hat Enterprise Linux - 4 years of updates 10.2 Red Hat Enterprise Linux - 4 years of updates 10.0 Red Hat Enterprise Linux - Extended Life Cycle 10.2 Red Hat Enterprise Linux 8 Red Hat Enterprise Linux - Extended Life Cycle 8.10 Red Hat CodeReady Linux Builder 10 Red Hat CodeReady Linux Builder - Extended Update Support 10.2 Red Hat CodeReady Linux Builder - Extended Update Support 10.0 Red Hat CodeReady Linux Builder 8 JBoss Enterprise Web Server Text-Only Advisories
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:39494 https://access.redhat.com/errata/RHSA-2026:39371 https://access.redhat.com/errata/RHSA-2026:39189 https://access.redhat.com/errata/RHSA-2026:39083

Vendor	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-14371, CVE-2026-10587, CVE-2026-10588, CVE-2026-10589, CVE-2026-10590, CVE-2026-25271, CVE-2026-6090, CVE-2026-6511, CVE-2026-20457, CVE-2026-20458, CVE-2026-20459, CVE-2026-20460, CVE-2026-20461, CVE-2026-20462, CVE-2026-20463)
Description	Lenovo 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. 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-220765 https://support.lenovo.com/us/en/product_security/LEN-220440 https://support.lenovo.com/us/en/product_security/LEN-218281 https://support.lenovo.com/us/en/product_security/LEN-217317

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-6237, CVE-2024-4741, CVE-2022-43680, CVE-2023-52425, CVE-2023-52426, CVE-2024-28757, CVE-2026-25210, CVE-2026-32776, CVE-2026-32777, CVE-2026-32778, CVE-2025-60876)
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	iDRAC9 Versions prior to 7.30.30.51 Multiple PowerEdge and XC Core Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000489258/dsa-2026-316-security-update-for-dell-poweredge-server-for-openssl-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000489193/dsa-2026-312-security-update-for-dell-idrac9-vulnerabilities

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-31685, CVE-2026-43025, CVE-2026-43037, CVE-2026-43190, CVE-2026-43437, CVE-2026-45970, CVE-2026-46243, CVE-2026-31758, CVE-2026-43501, CVE-2026-46120, CVE-2026-46173, CVE-2026-46227, CVE-2026-52909, CVE-2026-52943, CVE-2026-43366, CVE-2026-23393, CVE-2026-31505, CVE-2026-31533, CVE-2026-31570, CVE-2026-31586, CVE-2026-43027, CVE-2026-43494, CVE-2026-43120, CVE-2026-53362)
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 Linux Enterprise High Performance Computing 12 SP5, 15 SP4 and 15 SP5 • SUSE Linux Enterprise Live Patching 12-SP5, 15-SP4, 15-SP5, 15-SP6 and 15-SP7 • SUSE Linux Enterprise Micro 5.3, 5.4 and 5.5 • SUSE Linux Enterprise Real Time 15 SP4, 15 SP5, 15 SP6 and 15 SP7 • SUSE Linux Enterprise Server 12 SP5, 15 SP4, 15 SP5, 15 SP6 and 15 SP7 • SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP4, 15 SP5, 15 SP6 and 15 SP7 • openSUSE Leap 15.4, 15.5 and 15.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20262992-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262991-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262989-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262955-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262961-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262956-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262957-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262945-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262943-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262938-1/

Vendor	**Ivanti**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-14902, CVE-2026-14903, CVE-2024-13181, CVE-2024-13180, CVE-2024-13179)
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 Xtraction versions 2026.2 and prior Ivanti Avalanche versions 6.4.6 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Xtraction-CVE-2026-14902-CVE-2026-14903?language=en_US • https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-7-Multiple-CVEs?language=en_US

Vendor	**ASUS**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-11851, CVE-2026-15029, CVE-2026-15030, CVE-2026-13585)
Description	ASUS 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. ASUS advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	ASUS System Control Interface v3 earlier than v3.1.66.0 ASUS System Control Interface earlier than v1.1.40.0 ASUS Business Manager earlier than v3.0.38.0 ASUS router firmware: • 3.0.0.4_386 series • 3.0.0.4_388 series • 3.0.0.6_102 series
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.asus.com/security-advisory

Vendor	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-40860, CVE-2026-40453, CVE-2026-33454, CVE-2026-0487, CVE-2026-44752, CVE-2026-44745, CVE-2026-43512, CVE-2026-41293, CVE-2026-43515, CVE-2026-58233, CVE-2026-44759, CVE-2026-44767, CVE-2026-44769, CVE-2026-44760, CVE-2026-44771, CVE-2026-44770, CVE-2026-24315, CVE-2026-44768, CVE-2026-44753, CVE-2025-68161)
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 Integration Suite (Edge Integration Cell) versions prior to 8.43.11 • SAProuter on Windows — KRNL64NUC 7.22/7.22EXT, KRNL64UC 7.22/7.22EXT/7.53, SAP_ROUTER 7.53/7.54, KERNEL 7.22/7.53/7.54/7.77/7.89/7.93/9.16–9.18 • SAP NetWeaver AS Java (Configuration Wizard) LMCTC 7.50 • SAP NetWeaver AS Java — SERVERCORE 7.50, CORE-TOOLS 7.50, J2EE-APPS 7.50 • SAP NetWeaver AS ABAP (BSP-based applications) SAP_BASIS 700–758, 816, 918–920 • SAP Approuter (node.js) versions prior to 21.2.0 • SAP Commerce Cloud — HY_COM 2205, COM_CLOUD 2211/2211-JDK21 • SAP CTS Attach Tool (ctsattach) CTS_UPLOAD_CLT 1 • SAP NetWeaver Enterprise Portal EP-RUNTIME 7.50 • SAP S/4HANA Project Management (PPM-PRO) — SAP_APPL 600–606/617/618, S4CORE 102–108, CPRXRPM 400/450_700/500_702/610_740 • SAP S/4HANA (Draft Operation) S4CORE 108 • SAP S/4HANA (Create Single Payment) S4CORE 102–109 • SAP Fiori (Launchpad) SAP_UI 754–758, 816 • SAP CRM (WebClient UI) S4FND 104–106 • SAP HANA XS Classic (User Self Service) HDB 2.00 • UI5 Web Components (base) versions prior to 2.21.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/july-2026.html

Vendor	**Fortinet**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-43892, CVE-2026-59840, CVE-2026-59838, CVE-2025-62675, CVE-2025-62826, CVE-2026-59836, CVE-2025-53379, CVE-2026-59839, CVE-2026-23573, CVE-2026-59837, CVE-2026-59841, CVE-2026-59835)
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	FortiOS 6.4 – 7.4 (all versions), 7.6.0 through 7.6.6 FortiProxy 7.2 – 7.4 (all versions), 7.6.0 through 7.6.5 FortiSIEM 6.4 – 7.1 (all versions), 7.2.0 through 7.2.6, 7.3.0 through 7.3.4, 7.4.0 FortiClientEMS 7.2 (all versions), 7.4.0 through 7.4.1, 7.4.3 through 7.4.5 FortiAuthenticator 6.5.0 through 6.5.7, 6.6.0 through 6.6.2 FortiPAM 1.0 – 1.6 (all versions), 1.7.0 through 1.7.2, 1.8.0 FortiSIEMWindowsAgent 7.4.0 through 7.4.1 FortiSandbox 4.4.3 through 4.4.8, 5.0.0 through 5.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-26-154 https://www.fortiguard.com/psirt/FG-IR-26-149 https://www.fortiguard.com/psirt/FG-IR-26-152 https://www.fortiguard.com/psirt/FG-IR-26-153 https://www.fortiguard.com/psirt/FG-IR-26-147 https://www.fortiguard.com/psirt/FG-IR-26-146 https://www.fortiguard.com/psirt/FG-IR-26-151 https://www.fortiguard.com/psirt/FG-IR-26-150 https://www.fortiguard.com/psirt/FG-IR-26-148 https://www.fortiguard.com/psirt/FG-IR-26-155 https://www.fortiguard.com/psirt/FG-IR-26-145

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 QRadar Data Synchronization App versions 1.0.0 - 3.3.0 QRadar User Behavior Analytics versions 1.0.0 - 5.1.0 Disconnected Log Collector versions 1.0.0 - 2.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7279972 https://www.ibm.com/support/pages/node/7279973 https://www.ibm.com/support/pages/node/7279975

Vendor	**NETGEAR**	
Severity	**Medium**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-15757, CVE-2026-62655, CVE-2026-62656, CVE-2026-62657, CVE-2026-62658, CVE-2026-62659)	
Description	NETGEAR 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. NETGEAR advises to apply these security fixes at your earliest to protect your systems from potential threats.	
Affected Products	DGND3700v1 (EoS) RBE970 versions prior to V9.10.1.4 RBE971 versions prior to V9.10.1.4 RBR860 versions prior to V7.2.7.15 RBRE950 versions prior to v7.2.7.15 RBRE960 versions prior to V7.2.7.15 RBS860 versions prior to V7.2.7.15 RBSE950 versions prior to v7.2.7.15 RBSE960 versions prior to V7.2.7.15 RAXE450 versions prior to V1.2.14.114 RAXE500 versions prior to V1.2.14.114	MR70 versions prior to V1.0.4.48 MS70 versions prior to V1.0.4.48 RAXE500 versions prior to V1.2.14.114 XR1000 versions prior to V1.0.2.86 RAX43 (EoS) RAX45 (EoS) RAX50 versions prior to V1.0.17.142 RAX54S versions prior to V1.0.17.142 RAX54Sv2 versions prior to V1.1.6.36 WAX333 versions prior to V2.8.0.100
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://kb.netgear.com/000070859/July-2026-NETGEAR-Security-Advisory	

Vendor	**Citrix**
Severity	**Medium**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2026-42491)
Description	Citrix has released a security update addressing a vulnerability that exists in their products. **CVE-2026-42491:** An issue has been identified in the XenServer management API SDK that may allow an attacker on the management network who is able to intercept specific HTTPS requests within a higher-level operation to be able to act with the privileges of the intercepted administrator. Citrix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	XenCenter (versions prior to 2026.4.0) XenServer SDK for PowerShell and C# (versions prior to 26.15.0)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696811&articleURL=XenServer_Security_Update_for_CVE_2026_42491

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.