Advisory Alert

Alert Number: AAA20260812 **Date:** August 12, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
Commvault	**Critical**	Multiple Vulnerabilities
SonicWall	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Improper Validation Vulnerability
SAP	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Commvault	**High**	Server-Side Request Forgery (SSRF) Vulnerability
Lenovo	**High**	Multiple Vulnerabilities
Ivanti	**High**	Multiple Vulnerabilities
Cisco	**High**	Denial of Service Vulnerability
ASUS	**High**	Privilege Escalation Vulnerability
SonicWall	**High**, **Medium**	Multiple Vulnerabilities
Intel	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
SAP	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-15154, CVE-2026-15467, CVE-2026-15581, CVE-2026-16456, CVE-2026-16745, CVE-2026-18608, CVE-2026-18611, CVE-2026-18617, CVE-2026-18618, CVE-2026-18620, CVE-2026-18621, CVE-2026-18941, CVE-2026-18947, CVE-2026-18948, CVE-2026-18949, CVE-2026-18950, CVE-2026-18951, CVE-2026-18982, CVE-2026-13717, CVE-2026-14450, CVE-2026-18942)
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 OpenShift AI
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:53263 https://access.redhat.com/errata/RHSA-2026:53262 https://access.redhat.com/errata/RHSA-2026:53261

Vendor	**Commvault**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-13738, CVE-2026-13737)
Description	Commvault has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-13738:** CommServe contained an authorization bypass vulnerability affecting a limited set of command execution operations. Software customers upgrade to resolved maintenance release. Update all Commvault installations, including Commserve, Webserver, Command Center, Media Agents, Clients and HyperScale X. **CVE-2026-13737:** CommServe contained an allowlist bypass vulnerability affecting command execution authorization. Software customers upgrade to resolved maintenance release. Update all Commvault installations, including Commserve, Webserver, Command Center, Media Agents, Clients and HyperScale X. Commvault advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Commvault (Linux / Windows): • 11.36.0 – 11.36.113 • 11.40.0 – 11.40.62 • 11.44.0 – 11.44.10 • 11.46.0 – 11.46.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://documentation.commvault.com/securityadvisories/CV_2026_07_9.html https://documentation.commvault.com/securityadvisories/CV_2026_07_8.html

Vendor	**SonicWall**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-66145, CVE-2026-66146, CVE-2026-66147, CVE-2026-66148)
Description	SonicWall 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. SonicWall advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	GMS - Virtual Appliance and Windows versions 9.5.1 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0011

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Improper Validation Vulnerability (CVE-2026-34182)
Description	IBM has released a security update addressing a vulnerability that exists in their products. **CVE-2026-34182:** Cryptographic Message Services (CMS) processing fails to perform sufficient input validation on the cipher and tag length fields of AuthEnvelopedData containers, leading to various potential compromises. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Cloud Pak for Data System versions 1.0.0.0 - 1.0.10.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7283256

Vendor	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-58231, CVE-2026-44772, CVE-2026-34265, CVE-2026-44758)
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 Commerce Cloud (Data Hub Adapter) SAP Manufacturing Integration and Intelligence SAP NetWeaver and ABAP Platform
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/august-2026.html?isu_page=1

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 Container Isolation FS Filter	Windows Schannel

	Driver (unionfs.sys) Microsoft Azure Attestation service and Device Health Attestation Service Microsoft Office SharePoint .NET Windows Management Services Windows Installer Azure CycleCloud Microsoft Edge (Chromium-based) Microsoft PowerShell Microsoft PowerShell Core Visual Studio Code GitHub Copilot and Visual Studio Code Windows DNS Microsoft Office Outlook Microsoft Office Excel Microsoft Office PowerPoint Microsoft Office Microsoft Office Word Windows Ancillary Function Driver for WinSock Windows Package Manager Windows Network File System Windows Cross Device Service Windows Key Guard Microsoft Edge for Android Microsoft Dynamics 365 (on-premises) Windows Storage Port Driver Microsoft Exchange Server Power BI .NET Framework Windows iSCSI Target Service Windows SMB Client Windows Message Queuing Desktop Window Manager Windows DHCP Client Windows NTFS Windows Autopilot Windows Active Directory Windows Win32K Windows Kernel Microsoft Teams Mobile Microsoft Teams for Android Microsoft OneDrive Visual Studio Code CoPilot Chat Extension Microsoft Entra Connect Sync Windows Remote Access API Windows GDI Microsoft Office Access Windows Backup Engine Microsoft QUIC Windows DWM Core Library Windows Deployment Services Capability Access Management Service (camsvc) Windows GDI+ Windows Secure Socket Tunneling Protocol (SSTP) Windows User Profile Service Remote Desktop Client Windows DHCP Server Windows Routing and Remote Access Service (RRAS) Active Directory Certificate Services (AD CS) Reliable Multicast Transport Driver (RMCAST) Windows HTTP.sys Windows SMB Server Windows LDAP - Lightweight Directory Access Protocol Windows TCP/IP Microsoft Local Security Authority Server (lsasrv) Windows Remote Access Connection Manager RPC Runtime	Windows License Manager Windows Graphics Kernel Windows Kerberos Windows Cloud Files Mini Filter Driver Windows Shell Windows Projected File System Windows HTTP Protocol Stack Windows Telephony Service Windows Device Association Service Windows Imaging Component Windows Management Instrumentation Windows Wired AutoConfig Service Windows Common Log File System Driver Windows Bind Filter Driver User-Mode Power Service (UMPS) Windows Modern Device Management (MDM) Windows Universal Disk Format File System Driver (UDFS) Microsoft Digest Authentication Windows Program Compatibility Assistant Service Windows Storage Windows MIDI Service Module Windows Remote Desktop Services Windows Push Notifications Winlogon Windows Defender Firewall Service Windows Hello Windows USB Driver Windows Display Enhancement Service Windows Hyper-V Windows Network Connection Broker Windows Accessibility Infrastructure (ATBroker.exe) Application Information Services Windows Sensor Data Service Windows Work Folder Service Windows Event Logging Service Microsoft Remote Registry Service Microsoft COM for Windows Microsoft Windows Search Component Microsoft High Performance Computing (HPC) Pack AMD Zen Windows Encrypting File System (EFS) Virtual Hard Disk (VHD) Miniport Driver Windows Terminal Windows Admin Center Azure Storage Explorer Windows Network Address Translation (NAT) Windows Narrator Braille Windows RDP Visual Studio Code - Python extension Microsoft Defender for Endpoint Azure Active Directory Active Directory Federation Services (AD FS) Windows LUAFV Windows Brokering File System Windows Resilient File System (ReFS) Windows DirectX Microsoft Install Service Windows Spaceport.sys Copilot Chat (Microsoft Edge) ASP.NET Core Microsoft Configuration Manager Azure Monitor Agent Windows RPC API Dynamics Business Central Windows PowerShell Microsoft Dynamics 365 Dynamics Business Central Control
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-2025-14813, CVE-2026-0636, CVE-2026-3505, CVE-2026-5588, CVE-2026-5598, CVE-2026-10579, CVE-2026-27446, CVE-2026-41417, CVE-2026-42578, CVE-2026-42579, CVE-2026-42581, CVE-2026-42584, CVE-2026-42585, CVE-2026-42587, CVE-2026-44249, CVE-2026-44250, CVE-2026-44890, CVE-2026-44893, CVE-2026-45416, CVE-2026-45674, CVE-2026-46340, CVE-2026-47691, CVE-2026-48006, CVE-2026-48043, CVE-2026-48059, CVE-2026-50010, CVE-2026-50011, CVE-2026-68494, CVE-2024-53143, CVE-2025-71072, CVE-2026-23415, CVE-2026-31488, CVE-2026-52923, CVE-2026-64368, CVE-2026-64531, CVE-2025-54518, CVE-2026-31530, CVE-2026-43112, CVE-2026-53264)
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	JBoss Enterprise Application Platform 7.4 ELS 7 x86_64 Red Hat Enterprise Linux 9 Base & CodeReady Builder: x86_64, aarch64, ppc64le, s390x Red Hat Enterprise Linux 9.6 (Extended Update Support, Advanced Update Support, Update Services for SAP Solutions, Four Years of Updates, Extended Life Cycle, and CodeReady Linux Builder Extended Update Support): x86_64, aarch64, ppc64le, s390x Red Hat Enterprise Linux 9.8 (Extended Update Support, Update Services for SAP Solutions, Four Years of Updates, Extended Life Cycle, and CodeReady Linux Builder Extended Update Support): x86_64, aarch64, ppc64le, s390x Red Hat Enterprise Linux 10 Base & CodeReady Builder: x86_64, aarch64, ppc64le, s390x Red Hat Enterprise Linux 10.2 (Extended Update Support, Four Years of Updates, Extended Life Cycle, and CodeReady Linux Builder Extended Update Support): x86_64, aarch64, ppc64le, s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:53990 https://access.redhat.com/errata/RHSA-2026:53329 https://access.redhat.com/errata/RHSA-2026:53330 https://access.redhat.com/errata/RHSA-2026:53806

Vendor	**Commvault**
Severity	**High**
Affected Vulnerability	Server-Side Request Forgery (SSRF) Vulnerability (CVE-2026-13739)
Description	Commvault has released a security update a vulnerability that exists in their products. **CVE-2026-13739:** A legacy endpoint in Command Center contained an unauthenticated server-side request forgery (SSRF) vulnerability related to the handling of arbitrary target URLs. Software customers upgrade to resolved maintenance release. Update Command Center. Commvault advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Commvault (Linux / Windows): • 11.46.0 - 11.46.9 • 11.44.0 - 11.44.10 • 11.40.0 - 11.40.62 • 11.36.0 - 11.36.113
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://documentation.commvault.com/securityadvisories/CV_2026_07_5.html

Vendor	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-31356, CVE-2025-31936, CVE-2025-31938, CVE-2025-35973, CVE-2026-6484, CVE-2026-6923, CVE-2026-20705, CVE-2026-20707, CVE-2026-20712, CVE-2026-20713, CVE-2026-20716, CVE-2026-20760, CVE-2026-20775, CVE-2026-20885, CVE-2026-20898, CVE-2026-20901, CVE-2026-20917)
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-222658

Vendor	**Ivanti**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-18129, CVE-2026-18127, CVE-2026-18125)
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 Endpoint Manager (EPM) versions 2024 SU6 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-EPM-August-2026?language=en_US

Vendor	**Cisco**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2026-20349)
Description	Cisco has released security updates addressing a vulnerability that exists in their products. **CVE-2026-20349:** A vulnerability in the Remote Access SSL VPN service for Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Secure FMC Software Cisco Secure Firewall ASA Software Cisco Secure FTD Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-dos-dzv4mQFF

Vendor	**ASUS**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2026-8917)
Description	ASUS has released a security update addressing a vulnerability that exists in their products. **CVE-2026-8917:** Untrusted Pointer Dereference in ASUS GPU Tweak III, GPUTweakII, AI Suite3, and VGAdll: An IOCTL vulnerability allows a local attacker to write a specific value to an arbitrary memory address, potentially leading to privilege escalation ASUS advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ASUS GPU Tweak III: v2.1.1.7 and earlier ASUS GPU Tweak II: v2.4.0.0 and earlier ASUS AI Suite 3: v2.1.2.0 and earlier ASUS VGA.dll (Armoury Crate component): v0.0.7.8 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.asus.com/security-advisory

Vendor	**SonicWall**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-0516, CVE-2026-66149, CVE-2026-66150)
Description	SonicWall 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. SonicWall advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Gen6 Hardware Firewalls (SOHO/W, SOHO 250/250W, TZ 300/300P/300W/350/350W/400/400W/500/500W/600/600P, NSa 2650/3600/3650/4600/4650/5600/5650/6600/6650, SM 9200/9250/9400/9450/9600/9650) • Affected Firmware: 6.5.5.2-28n and earlier Gen6 Virtual Firewalls (NSv) (NSv 10, 25, 50, 100, 200, 300, 400, 800, 1600) • Affected Firmware: 6.5.4.4-44v-21-2472 and earlier Gen7 Hardware & Virtual Firewalls (NSv) (TZ 270/270W/370/370W/470/470W/570/570W/570P/670, NSa 2700/3700/4700/5700/6700, NSsp 10700/11700/13700/15700, NSv 270/470/870 across ESXi, KVM, Hyper-V, AWS, Azure) • Affected Firmware: 7.0.1-5169 and earlier | 7.3.3-7015 and earlier Gen8 Hardware Firewalls (TZ 80/280/280W/380/380W/480/580/680, NSa 2800/3800/4800/5800) • Affected Firmware: 8.2.1-8010 and earlier SonicWall Email Security (Hardware Appliances 5000, 5050, 7000, 7050, 9000 & VMware / Hyper-V Virtual) • Affected Firmware: 10.0.35.8405 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0009 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0012

Vendor	**Intel**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20713, CVE-2026-20901, CVE-2026-20760, CVE-2026-20712, CVE-2026-20716, CVE-2025-35973, CVE-2026-20715, CVE-2026-20708, CVE-2026-20734, CVE-2025-31936, CVE-2026-6726, CVE-2026-6727)
Description	Intel 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. Intel 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://www.intel.com/content/www/us/en/security-center/default.html

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-9762, CVE-2026-25645, CVE-2026-7246, CVE-2026-44405, CVE-2026-44431, CVE-2026-44432, CVE-2026-45409, CVE-2026-9375, CVE-2026-21925, CVE-2026-21933, CVE-2026-34180, CVE-2026-34181, CVE-2026-34183, CVE-2026-42764, CVE-2026-42766, CVE-2026-42767, CVE-2026-42768, CVE-2026-42769, CVE-2026-42770, CVE-2026-45445, CVE-2026-45446, CVE-2026-7383, CVE-2026-9076, CVE-2026-5795, CVE-2026-45447)
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 Cloud Pak for Data System versions 1.0.0.0 - 1.0.10.0 IBM QRadar App SDK versions 1.0.0 through 2.2.5 IBM Db2 11.5.0 - 11.5.9 and 12.1.0 - 12.1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7279479 https://www.ibm.com/support/pages/node/7283290 https://www.ibm.com/support/pages/node/7283256

Vendor	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-42947, CVE-2025-58057, CVE-2026-5598, CVE-2026-33871, CVE-2026-34480, CVE-2026-40130, CVE-2026-42945, CVE-2026-44762, CVE-2026-44763, CVE-2026-44764, CVE-2026-44765, CVE-2026-58230, CVE-2026-58233, CVE-2026-58235, CVE-2026-58236, CVE-2026-58237, CVE-2026-58238, CVE-2026-58239, CVE-2026-58241, CVE-2026-58243, CVE-2026-58244, CVE-2026-58245, CVE-2026-58247, CVE-2026-58248, CVE-2026-66760, CVE-2026-66761, CVE-2026-66763, CVE-2026-66764, CVE-2026-66770, CVE-2026-66771, CVE-2026-66772, CVE-2026-66773, CVE-2026-66774, CVE-2026-66775, CVE-2026-66776, CVE-2026-66777, CVE-2026-66778, CVE-2026-66779)
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/august-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.