Advisory Alert

Alert Number: AAA20260610 **Date:** June 10, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Veeam	**Critical**	Remote Code Execution Vulnerability
Ivanti	**Critical**	Multiple Vulnerabilities
HPE	**Critical**	Multiple Vulnerabilities
Fortinet	**Critical**	OS Command Injection Vulnerability
SAP	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Memory Translation Bypass Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Ivanti	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
AMD	**High**	Multiple Vulnerabilities
IBM	**High**	Improper Access Control Vulnerability
Lenovo	**High**, **Medium**	Multiple Vulnerabilities
HPE	**High**, **Medium**	Multiple Vulnerabilities
OpenSSL	**High**, **Medium**, **Low**	Multiple Vulnerabilities
SAP	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Fortinet	**Medium**	Multiple Vulnerabilities
Netgear	**Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**Veeam**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2026-44963)
Description	Veeam has released a security update addressing a vulnerability that exists in their product. **CVE-2026-44963**: A vulnerability allowing remote code execution (RCE) on the Backup Server by an authenticated domain user. Veeam advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Veeam Backup & Replication 12.3.2.4465 and all earlier version 12 builds.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4869

Vendor	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-10520, CVE-2026-10523)
Description	Ivanti has released a security update addressing multiple vulnerabilities that exist in their product. **CVE-2026-10520**: An OS Command Injection vulnerability in Ivanti Sentry that allows a remote unauthenticated user to achieve root-level remote code execution **CVE-2026-10523**: An Authentication Bypass vulnerability in Ivanti Sentry before the R10.5.2, R10.6.2 and R10.7.1 versions allows a remote unauthenticated attacker to create arbitrary administrative accounts and obtain full administrative access Ivanti advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ivanti Sentry - Versions 10.5.1, 10.6.1, 10.7.0 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Sentry-CVE-2026-10520-CVE-2026-10523?language=en_US

Vendor	**HPE**
Severity	**Critical**
Affected Vulnerability	Memory Translation Bypass Vulnerability (CVE-2025-10263)
Description	HPE has a released security update addressing a vulnerability that exists in their product. **CVE-2025-10263**: A broadcast TLBI on another PE may complete before affected memory accesses are globally observed. This may permit bypass of Stage 1 translation and/or Stage 2 translation. The vulnerability could allow remote attackers to gain unintended access to protected memory regions, potentially leading to data leakage, privilege escalation, or system compromise. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE ProLiant RL300 Gen11 - Prior to 1.84_04-02-2026
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05057en_us&docLocale=en_US

Vendor	**Fortinet**
Severity	**Critical**
Affected Vulnerability	OS Command Injection Vulnerability (CVE-2026-25089)
Description	Fortinet has released a security update addressing a vulnerability that exists in their products. **CVE-2026-25089**: An improper neutralization of special elements used in an OS command vulnerability in FortiSandbox, FortiSandbox Cloud and FortiSandbox PaaS WEB UI may allow an unauthenticated attacker to execute unauthorized commands via specifically crafted HTTP requests. Fortinet advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• FortiSandbox 5.0 - Versions 5.0.0 through 5.0.5 • FortiSandbox 4.4 - Versions 4.4.0 through 4.4.8 • FortiSandbox Cloud 5.0 - 5.0.4 through 5.0.5 • FortiSandbox PaaS 5.0 - 5.0.4 through 5.0.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-26-141

Vendor	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-44748, CVE-2026-27671, CVE-2026-22732, 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 AS ABAP and ABAP Platform Versions: • SAP_BASIS: 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 758, 816, 918, 919 • KRNL64NUC: 7.22, 7.22EXT • KRNL64UC: 7.22, 722EXT, 7.53 • KERNEL: 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 9.16, 9.18, 91.9 SAP Commerce Cloud and SAP Data Hub Versions: • HY_COM: 2205 • HY_DHUB: 2205 • COM_CLOUD: 2211, 2211-JDK21 • DHUB_CLOUD: 2211 SAP NetWeaver Application Server Java (Web Container) Versions : • 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/june-2026.html

Vendor	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Microsoft has released security updates addressing multiple vulnerability that exists 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	Microsoft PC Manager Windows 10 Version 22H2 for x64-based Systems Windows Server 2016 (Server Core installation) .NET 8.0 installed on Mac OS, Linux & Windows ASP.NET Core 8.0 .NET 10.0 installed on Linux ASP.NET Core 10.0 Windows Server 2025 Windows 11 Version 24H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows 11 Version 23H2 for x64-based Systems Microsoft PowerPoint for Android Microsoft Excel for Android Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 & 2016 Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 11 Version 26H1 for ARM64-based Systems Windows 11 version 26H1 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 11 Version 25H2 for x64-based Systems Windows 11 Version 25H2 for ARM64-based Systems Windows Server 2025 (Server Core installation) Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows Server 2022 (Server Core installation) Windows Server 2022 Windows 11 Version 26H1 for x64-based Systems - extra Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows Server 2019 (Server Core installation) Windows Server 2019 Microsoft 365 Apps for Enterprise for 32 & 64-bit Systems Microsoft Office 2019 for 32 & 64-bit editions Microsoft Live Share Canvas SDK Microsoft Word for Android Remote Desktop client for Windows Desktop Microsoft Office 365 for Mac Microsoft Office LTSC for Mac 2024 Microsoft Office LTSC 2024 for 64-bit editions Microsoft Office LTSC 2024 for 32-bit editions Windows App Client for Windows Desktop Visual Studio Code Windows Narrator Braille Microsoft SharePoint Server Subscription Edition Microsoft SharePoint Server 2019 Microsoft SharePoint Enterprise Server 2016 Microsoft Exchange Server 2019 Cumulative Update 14 Microsoft Exchange Server 2016 Cumulative Update 23 Microsoft Office LTSC 2021 for 64-bit editions Microsoft Office LTSC for Mac 2021 Azure Stack Edge Microsoft Word 2016 (32 & 64-bit edition) Microsoft Office LTSC 2021 for 32-bit editions Microsoft Defender for Endpoint for Mac Azure Kubernetes Service .NET 10.0 installed on Mac OS .NET 10.0 installed on Windows Microsoft Visual Studio 2026 version 18.6 Microsoft Exchange Server Subscription Edition RTM Microsoft Exchange Server 2019 Cumulative Update 15 Microsoft Excel 2016 (32 &64-bit edition) ASP.NET Core 9.0 .NET 9.0 installed on Windows .NET 9.0 installed on Linux .NET 9.0 installed on Mac OS Microsoft Visual Studio Code CoPilot Chat Extension Linux kernel - Microsoft MANA Network Driver Microsoft Office 2016 (64-bit edition) Microsoft Office 2016 (32-bit edition) Microsoft Office for Android Office Online Server Microsoft Teams for Android Microsoft Dynamics 365 (on-premises) version 9.1 PowerScribe One version 2023.1 SP3 Patch 6 PowerScribe One version 2023.1 SP2 Patch 11 Nuance PowerScribe One version 2019.10 Nuance PowerScribe One version 2019.9 Nuance PowerScribe One version 2019.8 Nuance PowerScribe One version 2019.7 Nuance PowerScribe One version 2019.6 Nuance PowerScribe One version 2019.5 Nuance PowerScribe One version 2019.4 Nuance PowerScribe 360 version 4.0.4 Nuance PowerScribe 360 version 4.0.3 Nuance PowerScribe 360 version 4.0.2 Nuance PowerScribe 360 version 4.0.1 Nuance PowerScribe 360 4.0 Nuance PowerScribe One version 2019.3 Nuance PowerScribe One version 2019.2 Nuance PowerScribe One version 2019.1 Nuance PowerScribe 360 version 4.0.9 Nuance PowerScribe 360 version 4.0.8 Nuance PowerScribe 360 version 4.0.7 Nuance PowerScribe 360 version 4.0.6 Nuance PowerScribe 360 version 4.0.5 Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows Server, version 2004 (Server Core installation) Visual Studio Code - MSSQL Extension Microsoft Bing Search for Android .NET 8.0 Microsoft PowerToys Microsoft Exchange Online Microsoft Graph Copilot Chat (Microsoft Edge) Microsoft 365 Copilot Azure HorizonDB Microsoft Global Secure Access (GSA) Microsoft Entra ID Microsoft Planetary Computer Pro (GeoCatalog) Azure Stack HCI Microsoft 365 Copilot for iOS Azure Resource Manager Azure Virtual Network Gateway Azure Privileged Identity Management (PIM) Microsoft Power Pages Azure Orbital Spatio Windows Admin Center in Azure Portal Microsoft Malware Protection Engine Microsoft Defender Antimalware Platform Azure Local Microsoft Edge (Chromium-based) Microsoft Authenticator for IOS Microsoft Authenticator for Android
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2026-9311)
Description	IBM has released a security update addressing a vulnerability that exist in their products. **CVE-2026-9311**: IBM WebSphere Application Server 9.0, and 8.5 is vulnerable to remote code execution caused by the bypass of security controls. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Cloud Pak for Applications Version: • 5.1, 5.2 & 5.3 IBM WebSphere Application Server Versions: • 9.0.0.0 - 9.0.5.28 • 8.5.5.0 - 8.5.5.29
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7275615

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-46300, CVE-2026-46333)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-46300**: A flaw was found in the Linux kernel's XFRM ESP-in-TCP subsystem. Unsafe in-place cryptographic processing allows a low-privileged local attacker to write arbitrary bytes into the page cache of read-only files, including sensitive system files. An attacker can exploit this to overwrite privileged binaries and gain root privileges. **CVE-2026-46333**: A vulnerability was found in the Linux kernel that allows an unprivileged local user to read sensitive files normally restricted to the root user. The flaw occurs during process exit, where a brief window allows an attacker to intercept file access from a privileged process before it fully terminates. Successful exploitation may lead to the disclosure of sensitive data such as SSH host private keys or /etc/shadow contents. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Red Hat Enterprise Linux Server - AUS 9.4 x86_64 • Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le • Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.4 x86_64 • Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:24814

Vendor	**Ivanti**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-6973, CVE-2026-10727)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-6973**: A configuration control vulnerability in the Ivanti Endpoint Manager Mobile before 12.9.0.1, 12.8.0.3 and 12.7.0.2 versions allows a remote authenticated attacker to inject arbitrary Apache directives, leading to remote code execution. **CVE-2026-10727**: An OS command injection vulnerability in Ivanti EPMM before 12.9.0.1, 12.8.0.3 and 12.7.0.2 versions allows a remote authenticated attacker to execute arbitrary commands as root Ivanti advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ivanti Endpoint Manager Mobile - Versions 12.9.0, 12.8.0.2, 12.7.0.1 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-6973-CVE-2026-10727?language=en_US

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-31405, CVE-2026-31473, CVE-2026-31613, CVE-2026-31614, CVE-2026-31629, CVE-2026-31758, CVE-2026-43037, CVE-2026-43206, CVE-2026-43284, CVE-2026-43362, CVE-2026-43499, CVE-2026-43501, CVE-2026-43503, CVE-2026-45852, CVE-2026-45910, CVE-2026-45970, CVE-2026-46004, CVE-2026-46021, CVE-2026-46043, CVE-2026-46113, CVE-2026-46114, CVE-2026-46243)
Description	SUSE 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. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.6 SUSE Linux Enterprise High Availability Extension 15 SP6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server 15 SP6 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20262310-1/

Vendor	**AMD**
Severity	**High**
Affected Vulnerability	Improper Access Control Vulnerability (CVE-2025-54509)
Description	AMD has released a security update addressing a vulnerability that exists in their products. **CVE-2025-54509:** Improper access control for register interface in the input-output memory management unit (IOMMU) could allow a privileged attacker to cause non-coherent accesses by the AMD Secure Processor (ASP) potentially resulting in loss of integrity. AMD advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	AMD EPYC™ Processors: • AMD EPYC™ 8004 Series Processors • AMD EPYC™ 9004 Series Processors • AMD EPYC™ 9005 Series Processors AMD EPYC™ Embedded Processors • AMD EPYC™ Embedded 8004 Series Processors • AMD EPYC™ Embedded 9004 Series Processors • AMD EPYC™ Embedded 9004 Series Processors • AMD EPYC™ Embedded 9005 Series Processors
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-3039.html

Vendor	**IBM**
Severity	**High**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2026-9330)
Description	IBM has released a security update addressing a vulnerability that exists in their products. **CVE-2026-9330**: IBM WebSphere Application Server 9.0, and 8.5 is affected by an improper validation of user-supplied data during deserialization using the SAML Web Single Sign-On component. This could result in remote code execution via a crafted HTTP request when combined with a suitable gadget chain. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Cloud Pak for Applications Version: • 5.1, 5.2 & 5.3 IBM WebSphere Application Server Versions: • 9.0.0.0 - 9.0.5.28 • 8.5.5.0 - 8.5.5.29
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7275615

Vendor	**Lenovo**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-10237, CVE-2025-10238, CVE-2025-54509, CVE-2026-20452, CVE-2026-20456, CVE-2025-20070, CVE-2025-22849)
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-218282 • https://support.lenovo.com/us/en/product_security/LEN-216077 • https://support.lenovo.com/us/en/product_security/LEN-194481

Vendor	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-54509, CVE-2026-42945)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-54509**: A potential security vulnerability has been identified in certain HPE ProLiant DL servers using certain AMD EPYC processors. This vulnerability could be locally exploited to compromise system integrity. **CVE-2026-42945**: A vulnerability in the ngx_http_rewrite_module of NGINX Plus and NGINX Open Source may allow a remote unauthenticated attacker to trigger a heap buffer overflow using crafted HTTP requests under specific configuration conditions. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE ProLiant Servers: • HPE ProLiant Compute DL325 Gen12 - Prior to 1.40_01-09-2026 • HPE ProLiant Compute DL345 Gen12 - Prior to 1.40_01-09-2026 • HPE ProLiant DL145 Gen11 - Prior to 1.80_02-06-2026 • HPE ProLiant DL325 Gen11 Server - Prior to 3.00_02-06-2026 • HPE ProLiant DL345 Gen11 Server - Prior to 3.00_02-06-2026 • HPE ProLiant DL365 Gen11 Server - Prior to 3.00_02-06-2026 • HPE ProLiant DL385 Gen11 Server - Prior to 3.00_02-06-2026 HPE Aruba Networking • Management Software (Airwave): 8.3.0.6 and below. • Private 5G Management Dashboard: All supported versions.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05064en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05065en_us&docLocale=en_US

Vendor	**OpenSSL**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-34180, CVE-2026-34181, CVE-2026-34182, CVE-2026-34183, CVE-2026-35188, CVE-2026-42764, CVE-2026-42765, CVE-2026-42766, CVE-2026-42767, CVE-2026-42768, CVE-2026-42769, CVE-2026-42770, CVE-2026-42771, CVE-2026-45445, CVE-2026-45446, CVE-2026-45447, CVE-2026-7383, CVE-2026-9076)
Description	OpenSSL 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. OpenSSL advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	OpenSSL Versions: • from 4.0.0 before 4.0.1 • from 3.6.0 before 3.6.3 • from 3.5.0 before 3.5.7 • from 3.4.0 before 3.4.6 • from 3.0.0 before 3.0.21 • from 1.1.1 before 1.1.1zh • from 1.0.2 before 1.0.2zq
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://openssl-library.org/news/vulnerabilities/

Vendor	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-29145, CVE-2025-66614, CVE-2026-24734, CVE-2026-44751, CVE-2026-44754, CVE-2026-44744, CVE-2026-44746, CVE-2026-44757, CVE-2026-44750, CVE-2026-44755, CVE-2026-24315, CVE-2026-44743, 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 Commerce Cloud: • HY_COM: 2205 • COM_CLOUD: 2211, 2211-JDK21 SAP NetWeaver AS ABAP and ABAP: • SAP_BASIS: 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 758, 816 ODP Data Replication APIs: • DW4CORE: 200, 300, 400 • PI_BASIS: 2006_1_700, 701, 702, 731, 740 • SAP_BW: 750, 816 SAP S/4HANA Versions: • S4FND: 102, 103, 104, 105, 106, 107, 108, 109 SAP NetWeaver AS Java (JDBC Test Servlet): • BI_UDI 7.50 SAP Wily Introscope Enterprise Manager: • WILY_INTRO_ENTERPRISE 10.8 SAP MDG (Review Match Groups Application): • S4CORE: 108 • SAP_BASIS: 916, 917 • SAP_ABA: 816 SAP Business Objects Business Intelligence Platform Versions • ENTERPRISE: 430, 2025, 2027 SAP Fiori (launchpad): • SAP_UI: 754, 755, 756, 757, 758, 816 SAP NetWeaver AS Java: • SERVERCORE: 7.50 • CORE-TOOLS: 7.50 • J2EE-APPS: 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/june-2026.html

Vendor	**Fortinet**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-67862, CVE-2026-49938)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-67862**: An Internal Asset Exposed to Unsafe Debug Access Level or State vulnerability in FortiOS and FortiProxy may allow an authenticated admin to execute lua scripts via crafted CLI commands. **CVE-2026-49938**: An improper access control vulnerability in FortiPortal API endpoints may allow a remote privileged attacker with organization user role to obtain sensitive network configuration data via crafted HTTP requests. Fortinet advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• FortiOS 7.6 - Versions 7.6.0 through 7.6.2 • FortiOS 7.4 - Versions 7.4.0 through 7.4.7 • FortiOS 7.2 - Versions 7.2.0 through 7.2.10 • FortiProxy 7.6 - Versions 7.6.0 through 7.6.3 • FortiProxy 7.4 - versions 7.4.0 through 7.4.10 • FortiProxy 7.2 - Versions 7.2.0 through 7.2.14 • FortiPortal 7.4 - Versions 7.4.0 through 7.4.7 • FortiPortal 7.2 - Versions 7.2.0 through 7.2.8 • FortiPortal 7.0 - 7.0 all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.fortiguard.com/psirt/FG-IR-26-143 • https://www.fortiguard.com/psirt/FG-IR-26-140

Vendor	**Netgear**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-9213, CVE-2026-9212, CVE-2026-9211, CVE-2026-3088, CVE-2026-9210, CVE-2026-0409, CVE-2026-0420, CVE-2026-0419, CVE-2026-0418, CVE-2026-0415, CVE-2026-0414, CVE-2026-0413, CVE-2026-0412, CVE-2026-0417, CVE-2026-0416, CVE-2026-0411, CVE-2026-0410)
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	MR/MS Series: • MR60, MR70, MR80, MS60, MS70, MS80 R Series: • R6400v2, R6700v3, R6700AX, R6900P, R7000, R7000P, R7960P, R8000P, R8500 RAX Series: • RAX5, RAX10, RAX10v2, RAX15, RAX20, RAX35, RAX35v2, RAX36S, RAX38, RAX38v2, RAX40, RAX40v2, RAX41, RAX41v2, RAX42, RAX42v2, RAX43, RAX43v2, RAX45, RAX48, RAX49S, RAX50, RAX50S, RAX50v2, RAX54Sv2, RAX54v2, RAX70, RAX75, RAX78, RAX80, RAX120, RAX120v1, RAX120v2, RAX200 RAXE Series: • RAXE300, RAXE450, RAXE500 RBE/RBR/RBS Series: • RBE37X, RBE77X, RBE97x, RBE970, RBE971, RBR10, RBR20, RBR350, RBR40, RBR50, RBR750, RBR760, RBR840, RBR850, RBR860, RBRE950, RBRE960, RBS10, RBS20, RBS350, RBS40, RBS50, RBS750, RBS760, RBS840, RBS850, RBS860, RBSE950, RBSE960 Other: • CAX30, CBR750, EX3700, EX3800, EX6120, EX6130, JR6150, LBR1020, LBR20, Orbi 370 (RBE370, RBE371, RBE372, RBE374), R9000, RAX30, RS700, XR450, XR500, XR1000, XR1000v2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.netgear.com/000070811/June-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.