Advisory Alert

Alert Number: AAA20261111 **Date:** November 11, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
Synology	**Critical**	Multiple Vulnerabilities
Ivanti	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
SAP	**Critical**	Multiple Vulnerabilities
Fortinet	**Critical**	Multiple Vulnerabilities
MongoDB	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Synology	**High**	Multiple Vulnerabilities
Lenovo	**High**	Multiple Vulnerabilities
WatchGuard	**High**	Local Privilege Escalation Vulnerability
Citrix	**High**	Multiple Vulnerabilities
IBM	**High**	Prototype Pollution Vulnerability
Ivanti	**High**, **Medium**	Multiple Vulnerabilities
HPE	**High**, **Medium**	Multiple Vulnerabilities
Fortinet	**High**, **Medium**	Multiple Vulnerabilities
SAP	**High**, **Medium**, **Low**	Multiple Vulnerabilities
AMD	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Netgear	**Medium**	Authentication Vulnerability
Dell	**Medium**	Multiple Vulnerabilities
OpenSSL	**Low**	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-47273, CVE-2026-16313, CVE-2026-28390, CVE-2026-34182, CVE-2026-42011, CVE-2026-42013, CVE-2026-43114, CVE-2026-45445, CVE-2026-45447, CVE-2026-55653, CVE-2026-59995, CVE-2026-59999, CVE-2026-60002, CVE-2026-64564, CVE-2026-68121, CVE-2026-80792, CVE-2026-86138, CVE-2026-86140, CVE-2026-86142, CVE-2026-86143, CVE-2026-86144, CVE-2026-86145, CVE-2026-89161, CVE-2026-89846, CVE-2026-98432, CVE-2026-99999, CVE-2026-103111, CVE-2026-111497, CVE-2026-114406)
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 Platform & Enterprise Software: • Red Hat OpenShift Container Platform 4.13 (RHEL 8 / 9): aarch64, ppc64le, s390x, x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:95745

Vendor	**Synology**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76954, CVE-2026-85101)
Description	Synology has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-76954:** An improper neutralization of special elements used in an SQL command vulnerability in the Auth API in Synology DiskStation Manager (DSM) before 7.2.1-69057-13, 7.2.2-72806-10, 7.3.2-86009-5, and 7.4.1-90080-1 allows remote attackers to read or write arbitrary files and conduct denial-of-service attacks. **CVE-2026-85101:** An authentication bypass using an alternate path or channel vulnerability in the rsync in Synology DiskStation Manager (DSM) before 7.2.1-69057-13, 7.2.2-72806-10, 7.3.2-86009-5, and 7.4.1-90080-1 allows remote attackers to read specific files, write arbitrary files, and conduct limited denial-of-service attacks. Synology advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• DSM 7.4 prior to 7.4.1-90080-1 • DSM 7.3 prior to 7.3.2-86009-5 • DSM 7.2.2 prior to 7.2.2-72806-10 • DSM 7.2.1 prior to 7.2.1-69057-13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_26_19

Vendor	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-121653, CVE-2026-121683)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-121653:** SQL injection in the Core of Ivanti Endpoint Manager before version 2024 SU8 allows a remote unauthenticated attacker to achieve remote code execution. **CVE-2026-121683:** Missing authentication in Ivanti Cloud Services Application version 5.0.8 allows a remote unauthenticated attacker to add and delete arbitrary trusted EPM Core certificate entries. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Ivanti Endpoint Manager (EPM) versions 2024 SU7 and prior • Ivanti Cloud Services Application (CSA) version 5.0.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-EPM-November-2026?language=en_US • https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-CVE-2026-121683?language=en_US

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-23450, CVE-2026-111497)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2021-23450:** All versions of package dojo are vulnerable to Prototype Pollution via the setObject function. **CVE-2026-111497:** A buffer overflow vulnerability in the Brotli decoder (c/dec/decode.c) in Google Brotli versions 1.0.3 through 1.2.0 on all platforms allows a remote unauthenticated attacker to corrupt adjacent decoder state memory, disclose sensitive memory contents, cause a denial of service, or potentially execute arbitrary code using a crafted Brotli-compressed stream. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• WebSphere Service Registry and Repository version 8.5 • IBM QRadar SIEM: 7.5.0 – 7.5.0 UP16 IF02 and 7.6.0.0 – 7.6.0.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7296000 https://www.ibm.com/support/pages/node/7295464

Vendor	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76964, CVE-2026-89126, CVE-2026-89103, CVE-2026-120017, CVE-2026-109803, CVE-2026-76965, CVE-2026-109795, CVE-2026-89119, CVE-2026-109798)
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/november-2026.html?isu_page=1

Vendor	**Fortinet**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-126257, CVE-2026-126253, CVE-2026-126156, CVE-2026-126229, CVE-2026-126261, CVE-2026-126147, CVE-2026-126164, CVE-2026-126148, CVE-2026-126251, CVE-2026-126155)
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-26-271 https://www.fortiguard.com/psirt/FG-IR-26-267 https://www.fortiguard.com/psirt/FG-IR-26-208 https://www.fortiguard.com/psirt/FG-IR-26-244 https://www.fortiguard.com/psirt/FG-IR-26-275 https://www.fortiguard.com/psirt/FG-IR-26-199 https://www.fortiguard.com/psirt/FG-IR-26-216 https://www.fortiguard.com/psirt/FG-IR-26-200 https://www.fortiguard.com/psirt/FG-IR-26-265 https://www.fortiguard.com/psirt/FG-IR-26-207

Vendor	**MongoDB**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-118383, CVE-2026-120808)
Description	MongoDB has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-118383:** A use-after-free in the replication component of MongoDB Server can occur when a newly elected replica set primary completes catch-up. The condition can be caused by requests that do not require authentication, and may result in the server terminating unexpectedly or, under certain conditions, arbitrary code execution in the context of the server process. **CVE-2026-120808:** An issue exists in MongoDB's macOS TLS client implementation where certificate chain-of-trust validation is bypassed for outbound connections to IPv6-addressed peers. When a MongoDB process using the Apple SecureTransport TLS backend connects to an IPv6 target, the trust evaluation result from SecTrustEvaluate is silently discarded, regardless of whether the peer's certificate is trusted. MongoDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	MongoDB Server versions: • 4.4: 4.4.0 prior to 4.4.32 • 5.0: 5.0.0 prior to 5.0.35 • 6.0: 6.0.0 prior to 6.0.30 • 7.0: 7.0.0 prior to 7.0.48 • 8.0: 8.0.0 prior to 8.0.37 • 8.3: 8.3.0 prior to 8.3.16 • 9.0: 9.0.0 prior to 9.0.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.mongodb.com/resources/products/alerts#security

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

Microsoft.DotNet.Web.ProjectTemplates.11.0	.NET 11.0 installed on Linux
Microsoft.DotNet.Web.ProjectTemplates.10.0	Aspire.Cli
Microsoft.DotNet.Web.ProjectTemplates.9.0	Azure Web Apps
Microsoft.DotNet.Web.ProjectTemplates.8.0	Windows Sandbox
Aspire Dashboard	Windows Server 2012 R2 (Server Core installation)
Aspire.Hosting.AppHost	Windows Server 2012
Aspire.Hosting	Windows Server 2012 R2
.NET 9.0 installed on Windows	Windows Server 2012 (Server Core installation)
.NET 8.0 installed on Mac OS	Windows Admin Center
.NET 9.0 installed on Linux	Azure DevOps Server 2025
.NET 9.0 installed on Mac OS	Microsoft Malware Protection Engine
.NET 11.0 installed on Mac OS	Azure Confidential Clean Room
.NET 10.0 installed on Mac OS	Microsoft HPC Pack 2016
Microsoft.AspNetCore.Server.HttpSys	Microsoft HPC Pack 2019
Microsoft Office LTSC for Mac 2024	kernel-mshv-6.6.137.mshv2-2.azl3.x86_64
Microsoft Office LTSC 2024 for 64-bit editions	.NET 10.0 installed on Windows
Microsoft Office LTSC 2021 for 32-bit editions	Microsoft Exchange Server Subscription Edition RTM
Microsoft Office LTSC 2021 for 64-bit editions	.NET 8.0 installed on Windows
Microsoft Office 365 for Mac	Microsoft Visual Studio 2026 version 18.12
Microsoft 365 Apps for Enterprise for 32-bit Systems	Microsoft.AspNetCore.WebUtilities
Microsoft 365 Apps for Enterprise for 64-bit Systems	Microsoft.Extensions.Validation
Microsoft Office LTSC 2024 for 32-bit editions	System.Formats.Cbor
Microsoft Office LTSC for Mac 2021	Microsoft Visual Studio 2026 version 18.11
Microsoft SharePoint Server Subscription Edition	Azure Privileged Identity Management (PIM)
Office Online Server	aznfs
Windows Server 2022	Azure Open AI
Microsoft SQL Server 2017 for x64-based Systems (CU31)	Azure DevOps
Microsoft SQL Server 2025 for x64-based Systems (GDR)	Azure DevOps Server
Windows Server 2025 (Server Core installation)	Azure Managed Grafana
Windows 10 Version 1809 for x64-based Systems	Azure CycleCloud 8.9.2
Microsoft SQL Server 2022 for x64-based Systems (CU27)	Microsoft Configuration Manager 2603
Microsoft SQL Server 2025 for x64-based Systems CU10	Microsoft Power Apps
Microsoft SQL Server 2019 for x64-based Systems (GDR)	Azure Front Door
Windows 11 version 26H1 for x64-based Systems	Microsoft JDBC Driver 13.4 for SQL Server
Windows 11 Version 26H2 for x64-based Systems	@azure/msal-node
Windows Server 2025	Microsoft Authentication Library for JavaScript
Windows 11 Version 26H1 for ARM64-based Systems	Microsoft Visual Studio 2022 version 17.14
Windows 11 Version 26H2 for ARM64-based Systems	Microsoft.DotNet.HotReload.Watch.Aspire
Windows 11 Version 25H2 for x64-based Systems	.NET 10.0 installed on Linux
Windows 11 Version 25H2 for ARM64-based Systems	Microsoft.AspNetCore.SignalR.StackExchangeRedis
Windows 11 Version 24H2 for x64-based Systems	.NET 8.0 installed on Linux
Windows 11 Version 24H2 for ARM64-based Systems	Microsoft.AspNetCore.Http.Connections
Windows 11 Version 23H2 for ARM64-based Systems	Azure CycleCloud 8.9.1
Windows 11 Version 23H2 for x64-based Systems	GitHub Copilot Plugin for JetBrains IDEs
Windows Server 2022 (Server Core installation)	Microsoft Agent Framework SDK - dotnet
Windows 10 Version 22H2 for x64-based Systems	mcp-gateway
Windows 10 Version 22H2 for ARM64-based Systems	Azure Machine Learning
Windows 10 Version 22H2 for 32-bit Systems	Microsoft Entra Private Network Connector
Windows 10 Version 21H2 for x64-based Systems	Microsoft.Data.SqlClient 7.0
Windows 10 Version 21H2 for 32-bit Systems	Microsoft.Data.SqlClient 7.1
Windows Server 2016 (Server Core installation)	Microsoft.Data.SqlClient 6.1
Windows 10 Version 21H2 for ARM64-based Systems	Azure Virtual Machines
Windows Server 2019	Azure Local
	HEVC Video Extensions for Licensed Applications
	Raw Image Extension
	HEVC Video Extensions
	HEVC Video Extensions from Device Manufacturer
	Microsoft.TestPlatform.CLI
	Microsoft GDK
	HEIF Image Extension
	Entra Device Registration
	Microsoft Edge (Chromium-based)
	Microsoft Visual Studio 2019 version 16.11
	Microsoft Visual Studio 2017 version 15.9
	.NET source-build Linux tarballs (all archive types)
	ASP.NET Core runtime and targeting-pack Linux tarballs (Microsoft-published)
	VM Inspector for Azure Virtual Machines
	Azure Kubernetes Configuration Service
	Microsoft Entra application proxy
	Azure Pipelines
	Azure AI Foundry
	Microsoft Exchange Online

	Windows 10 Version 1809 for 32-bit Systems Windows Server 2019 (Server Core installation) Windows Server 2016 Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Microsoft SQL Server 2019 for x64-based Systems (CU32) Microsoft SQL Server 2017 for x64-based Systems (GDR) Microsoft SQL Server 2022 for x64-based Systems (GDR) Microsoft SQL Server 2025 for x64-based Systems (CU9) Microsoft Teams for Android Azure File Sync v23 Microsoft.VisualStudio.Web.CodeGeneration.Design Microsoft.VisualStudio.Web.CodeGenerators.Mvc Microsoft.dotnet-scaffold Azure File Sync v22 Azure File Sync v21 Microsoft.dotnet-scaffold-aspnet Aspire.Dashboard.Sdk.linux-x64 PowerShell 7.6 Windows App Client for Windows Desktop PowerShell 7.7 Visual Studio Code .NET 11.0 installed on Windows System.Text.Json	Microsoft Identity Client for NodeJS microsoft-identity-web v3 microsoft-identity-web v4 Microsoft Visual Studio 2026 version 18.10
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
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: • Red Hat OpenShift Container Platform • Red Hat OpenShift Security Profiles Operator Red Hat Enterprise Linux 9: • Base & CRB 9: aarch64, ppc64le, s390x, x86_64 • 9.4: Advanced Update Support (AUS) (x86_64), Extended Life Cycle (all archs), 4 Years of Updates (aarch64, s390x), Update Services for SAP Solutions (ppc64le, x86_64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:98047 https://access.redhat.com/errata/RHSA-2026:97873 https://access.redhat.com/errata/RHSA-2026:97843 https://access.redhat.com/errata/RHSA-2026:95747 https://access.redhat.com/errata/RHSA-2026:95757 https://access.redhat.com/errata/RHSA-2026:96285 https://access.redhat.com/errata/RHSA-2026:95746 https://access.redhat.com/errata/RHSA-2026:95756 https://access.redhat.com/errata/RHSA-2026:96283

Vendor	**Synology**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Synology 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. Synology advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• DSM 7.4 prior to 7.4.1-90080-1 • DSM 7.3 prior to 7.3.2-86009-5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_26_18

Vendor	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20539, CVE-2023-20543, CVE-2023-31329, CVE-2024-21954, CVE-2024-21963, CVE-2024-36309, CVE-2024-36313, CVE-2024-36317, CVE-2024-36344, CVE-2024-36350, CVE-2024-36357, CVE-2025-0008, CVE-2025-0027, CVE-2025-29940, CVE-2025-29941, CVE-2025-48504, CVE-2025-52535, CVE-2025-52537, CVE-2025-54501, CVE-2025-54503, CVE-2025-54504, CVE-2025-54506, CVE-2025-54507, CVE-2025-54508, CVE-2025-61963, CVE-2025-62620, CVE-2025-62621, CVE-2025-62622, CVE-2025-66661, CVE-2025-66662, CVE-2026-0002, CVE-2026-0003, CVE-2026-0004, CVE-2026-0101, CVE-2026-0422, CVE-2026-0423, CVE-2026-0425, CVE-2026-0435, CVE-2026-0436, CVE-2026-0439, CVE-2026-0440, CVE-2026-0448, CVE-2026-0450, CVE-2026-0451, CVE-2026-0453, CVE-2026-0454, CVE-2026-0462, CVE-2026-0471, CVE-2026-0472, CVE-2026-0477, CVE-2026-0478, CVE-2026-0479, CVE-2026-0480, CVE-2026-97631, CVE-2026-14968, CVE-2026-18448, CVE-2026-25285, CVE-2026-28247, CVE-2026-28248, CVE-2026-28249, CVE-2026-40668, CVE-2026-40669, CVE-2026-40670, CVE-2026-40671, CVE-2026-40680)
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-231052

Vendor	**WatchGuard**
Severity	**High**
Affected Vulnerability	Local Privilege Escalation Vulnerability (CVE-2026-57907)
Description	WatchGuard has released a security update addressing a vulnerability that exists in their products. **CVE-2026-57907:** A privilege escalation vulnerability in WatchGuard Endpoint Protection's inter-process communication between the console and the protection service allows a local, low-privileged authenticated user to execute arbitrary code with SYSTEM privileges by injecting code into the trusted console process and issuing privileged commands to the service. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Endpoint Security (windows) versions >= 0 and < 8.00.26.0011
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.watchguard.com/CVE-2026-57907/

Vendor	**Citrix**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-102705, CVE-2026-102706, CVE-2026-102707, CVE-2026-102708, CVE-2026-119779, CVE-2026-119780, CVE-2024-21963, CVE-2024-36350, CVE-2024-36357, CVE-2026-0004)
Description	Citrix 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. Citrix advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• XenServer 8.4 • XenServer 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697316&articleURL=XenServer_Security_Update_for_Multiple_Issues

Vendor	**IBM**
Severity	**High**
Affected Vulnerability	Prototype Pollution Vulnerability (CVE-2020-5258)
Description	IBM has released a security update addressing a vulnerability that exists in their products. **CVE-2020-5258:** In affected versions of dojo (NPM package), the deepCopy method is vulnerable to Prototype Pollution. Prototype Pollution refers to the ability to inject properties into existing JavaScript language construct prototypes, such as objects. An attacker manipulates these attributes to overwrite, or pollute, a JavaScript application object prototype of the base object by injecting other values. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WebSphere Service Registry and Repository version 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7296000

Vendor	**Ivanti**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-18128, CVE-2026-105813, CVE-2026-105425, CVE-2026-105669, CVE-2026-123179, CVE-2026-123181, CVE-2026-105426, CVE-2026-105427, CVE-2026-107404, CVE-2026-107405, CVE-2026-83528)
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 Endpoint Manager (EPM) versions 2024 SU7 and prior • Ivanti User Workspace Manager (UWM) versions 2026.2 and prior • Ivanti Sentry versions 10.8.2, 10.7.3 and prior • Ivanti Endpoint Manager Mobile (EPMM) versions 12.10.0.0, 12.9.0.2 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-November-2026?language=en_US • https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-User-Workspace-Manager-CVE-2026-105813?language=en_US • https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Sentry-CVE-2026-105425-CVE-2026-105669-CVE-2026-123179-and-CVE-2026-123181?language=en_US • https://hub.ivanti.com/s/article/November-2026-Security-Advisory-Ivanti-EPMM-Multiple-CVEs?language=en_US

Vendor	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-36350, CVE-2026-36357, CVE-2025-0027, CVE-2025-52535, CVE-2025-62620, CVE-2025-29940, CVE-2025-52537, CVE-2025-54503, CVE-2025-54504, CVE-2025-54506, CVE-2025-54508, CVE-2025-62621, CVE-2026-33228, CVE-2026-49759, CVE-2026-95780, CVE-2026-95781, CVE-2026-95782, CVE-2026-95783, CVE-2026-95784, CVE-2026-95785, CVE-2026-95786)
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 Infrastructure: HPE Networking: • Private 5G Core (P5G Core): 1.26.1.4 and below • HPE ProLiant Compute & Servers: • DL145 Gen11: prior to v2.20_07-24-2026 • DL325 / DL345 / DL365 / DL385 Gen11 Series: prior to v3.20_07-24-2026 • DL325 Gen10 Plus, DL325 Gen10 Plus v2, DL345 Gen10 Plus, DL365 Gen10 Plus, DL385 Gen10 Plus v2:** prior to v4.20_09-17-2026 • DL325 Gen12 / DL345 Gen12: prior to v1.50_03-06-2026, 1.60_07-24-2026 • XD685: prior to v2.60_03-31-2026, 2.62_07-29-2026 • XL225n Gen10 Plus (1U Node) / XL645d Gen10 Plus / XL675d Gen10 Plus:** prior to v4.20_09-17-2026
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05180en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05181en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05179en_us&docLocale=en_US

Vendor	**Fortinet**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-126244, CVE-2025-61625, CVE-2026-126184, CVE-2026-126218, CVE-2026-126152, CVE-2026-126159, CVE-2026-126183, CVE-2026-121530, CVE-2026-126212, CVE-2026-126178, CVE-2026-126160, CVE-2026-126232, CVE-2026-126185, CVE-2026-126182, CVE-2026-126222, CVE-2026-126219, CVE-2026-126220, CVE-2026-126221, CVE-2026-126167, CVE-2026-126168, CVE-2026-126169, CVE-2026-126153, CVE-2026-126235, CVE-2026-126224, CVE-2026-126255, CVE-2026-126234, CVE-2026-126180, CVE-2026-126171, CVE-2026-126146, CVE-2026-126231, CVE-2026-126145, CVE-2026-126226, CVE-2026-126144, CVE-2026-126213, CVE-2026-126241, CVE-2026-126175, CVE-2026-126252, CVE-2026-126240, CVE-2026-126179, CVE-2026-126158, CVE-2026-126236, CVE-2026-126249, CVE-2026-126211, CVE-2026-126214, CVE-2026-126215, CVE-2026-126216, CVE-2026-126217)
Description	Fortinet 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. Fortinet 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.fortiguard.com/psirt

Vendor	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76966, CVE-2026-120008, CVE-2026-109800, CVE-2026-109799, CVE-2026-109793, CVE-2026-120010, CVE-2026-109806, CVE-2026-109807, CVE-2026-76970, CVE-2026-109804, CVE-2026-89114, CVE-2026-76973, CVE-2026-109794, CVE-2026-120013, CVE-2026-120012, CVE-2026-120015, CVE-2026-120009, CVE-2026-109797, CVE-2026-109802, CVE-2026-109811, CVE-2026-109801, CVE-2026-109809, CVE-2026-109805, CVE-2026-120016, CVE-2026-109810, CVE-2026-89125, CVE-2026-89129, CVE-2026-76976, CVE-2026-89128, CVE-2026-73635, CVE-2026-89115, CVE-2026-89131, CVE-2026-44768, CVE-2026-109808)
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/november-2026.html?isu_page=1

Vendor	**AMD**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20539, CVE-2026-0436, CVE-2024-36344, CVE-2024-36350, CVE-2024-36357, CVE-2024-36313, CVE-2026-40680, CVE-2026-48450, CVE-2026-0002, CVE-2026-0425, CVE-2025-61966, CVE-2025-61967, CVE-2025-61968, CVE-2026-0423, CVE-2026-0453, CVE-2024-36317, CVE-2025-66661, CVE-2026-0422, CVE-2025-61964, CVE-2025-66662, CVE-2026-0439, CVE-2026-0472, CVE-2025-62622, CVE-2026-0440, CVE-2026-0448, CVE-2026-0451, CVE-2026-0471, CVE-2026-0477, CVE-2026-0478, CVE-2026-0479, CVE-2025-61965, CVE-2025-0008, CVE-2026-14968, CVE-2024-21963, CVE-2026-0004, CVE-2024-36309, CVE-2023-20543, CVE-2023-31329)
Description	AMD 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. AMD 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.amd.com/en/resources/product-security/bulletin/amd-sb-3053.html https://www.amd.com/en/resources/product-security/bulletin/amd-sb-3057.html https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7073.html https://www.amd.com/en/resources/product-security/bulletin/amd-sb-4028.html https://www.amd.com/en/resources/product-security/bulletin/amd-sb-4018.html https://www.amd.com/en/resources/product-security/bulletin/amd-sb-3066.html

Vendor	**Netgear**
Severity	**Medium**
Affected Vulnerability	Authentication Vulnerability (CVE-2026-123180)
Description	Netgear has released a security update addressing a vulnerability that exists in their products. **CVE-2026-123180:** A missing authentication vulnerability in the RAX30 allows a network adjacent attacker who has authenticated to the WiFi network to obtain sensitive information and tamper with device configuration, including administrator credentials, without authenticating to the device. Netgear advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	RAX30 Nighthawk AX5 5-Stream AX2400 WiFi 6 Router version prior to v1.0.15.110
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.netgear.com/000070971/November-2026-NETGEAR-Security-Advisory

Vendor	**Dell**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-40705, CVE-2026-40426, CVE-2026-32672, CVE-2024-36357, CVE-2024-36350, CVE-2026-28235, CVE-2026-57884, CVE-2026-33270, CVE-2026-56438)
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000502736/dsa-2026-388-security-update-for-dell-client-platform-for-intel-npu-driver-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000507384/dsa-2026-414-security-update-for-dell-client-platform-for-multiple-amd-bios-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000530558/dsa-2026-497-security-update-for-dell-client-platform-for-an-amd-raid-configuration-driver-vulnerability • https://www.dell.com/support/kbdoc/en-us/000499184/dsa-2026-363-security-update-for-dell-client-platform-for-intel-graphics-advisory

Vendor	**OpenSSL**
Severity	**Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-95692, CVE-2026-95691, CVE-2026-88822, CVE-2026-107496, CVE-2026-88823)
Description	OpenSSL 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. OpenSSL advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	OpenSSL versions: • 1.0.2: 1.0.2 prior to 1.0.2zt • 1.1.1: 1.1.1 prior to 1.1.1zk • 3.0: 3.0.0 prior to 3.0.24 • 3.5: 3.5.0 prior to 3.5.10 • 4.0: 4.0.0 prior to 4.0.4 • 4.1: 4.1.0 prior to 4.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://openssl-library.org/news/vulnerabilities/

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.