Advisory Alert

Alert Number: AAA20260415 **Date:** April 15, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortinet	**Critical**	Multiple Vulnerabilities
SAP	**Critical**	SQL Command Injection Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Improper Neutralization of Escape, Meta, or Control Sequences Vulnerability
Synology	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Dell	**High, Medium**	Multiple Vulnerabilities
AMD	**High, Medium**	Multiple Vulnerabilities
Juniper Networks	**High, Medium**	Multiple Vulnerabilities
Fortinet	**High, Medium**	Multiple Vulnerabilities
HPE	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium, Low**	Multiple Vulnerabilities
SAP	**High, Medium, Low**	Multiple Vulnerabilities
Apache Tomcat	**Medium**	Multiple Vulnerabilities
NetApp	**Medium**	Improper Certificate Validation Vulnerability
Ivanti	**Medium**	Multiple Vulnerabilities
F5	**Low**	Use After Free Vulnerability

Description

Affected Product	**Fortinet**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-39813, CVE-2026-39808)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exists in their Storage Sentinel Product. **CVE-2026-39813**: A Path Traversal vulnerability [CWE-24] in FortiSandbox JRPC API may allow an unauthenticated attacker to bypass authentication via specially crafted HTTP requests. **CVE-2026-39808:** An Improper Neutralization of Special Elements used in an OS Command ('OS command injection') vulnerability [CWE-78] in FortiSandbox may allow an unauthenticated attacker to execute unauthorized code or commands via crafted HTTP requests. Fortinet advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiSandbox – Versions 4.4.0 through 4.4.8 FortiSandbox - Versions 5.0.0 through 5.0.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.fortiguard.com/psirt/FG-IR-26-112 • https://www.fortiguard.com/psirt/FG-IR-26-100

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	SQL Command Injection Vulnerability (CVE-2026-27681)
Description	SAP has released a security update addressing a vulnerability that exists in their product. **CVE-2026-27681**: Due to insufficient authorization checks in SAP Business Planning and Consolidation and SAP Business Warehouse, an authenticated user can execute crafted SQL statements to read, modify, and delete database data. This leads to a high impact on the confidentiality, integrity, and availability of the system. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SAP Business Planning and Consolidation and SAP Business Warehouse • HANABPC 810 • BPC4HANA 300 • SAP_BW 750, 752, 753, 754, 755, 756, 757, 758, 816
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2026.html

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Microsoft has released security update addressing multiple vulnerability that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected products Microsoft advises to apply security fixes at your earliest to protect systems from potential threats.

Affected Products

Microsoft .NET Framework 3.5 AND 4.7.2	
Microsoft .NET Framework 3.5 AND 4.8	.NET 8.0 installed on Windows
Microsoft .NET Framework 4.8	.NET 10.0 installed on Linux
Windows Server 2022 (Server Core installation)	.NET 10.0 installed on Mac OS
Windows Server 2022	.NET 10.0 installed on Windows
Windows Server 2012 R2 (Server Core installation)	Microsoft Visual Studio 2022 version 17.14
Microsoft Office LTSC 2021 for 64-bit editions	Microsoft Visual Studio 2022 version 17.12
Windows 11 Version 23H2 for x64-based Systems	Windows Admin Center
Windows 11 Version 23H2 for ARM64-based Systems	Microsoft Office 2016 (64-bit edition)
	Microsoft Office 2016 (32-bit edition)
Windows 11 Version 25H2 for x64-based Systems	Microsoft SharePoint Server Subscription Edition
Windows 11 Version 25H2 for ARM systems	
Windows Server 2025 (Server Core installation)	Microsoft SharePoint Server 2019
Windows 10 Version 22H2 for 32-bit Systems	Microsoft SharePoint Enterprise Server 2016
Windows 10 Version 22H2 for ARM64-based Systems	Microsoft PowerPoint 2016 (64-bit edition)
Windows 10 Version 22H2 for x64-based Systems	Microsoft PowerPoint 2016 (32-bit edition)
Windows 10 Version 21H2 for x64-based Systems	.NET 8.0
Windows 10 Version 21H2 for ARM64-based Systems	Microsoft HPC Pack 2019
	Remote Desktop client for Windows Desktop
Windows Server 2016 (Server Core installation)	
Windows Server 2016	Windows App Client for Windows Desktop
Windows 10 Version 1607 for x64-based Systems	Microsoft Power Apps
Windows 10 Version 1607 for 32-bit Systems	Microsoft Visual Studio Code CoPilot Chat Extension
Windows 10 Version 21H2 for 32-bit Systems	
Windows 10 Version 1809 for x64-based Systems	Microsoft Edge (Chromium-based)
Windows 10 Version 1809 for 32-bit Systems	Microsoft Edge for Android
Windows 11 version 26H1 for x64-based Systems	Microsoft Excel for iOS
Windows 11 Version 26H1 for ARM64-based Systems	Microsoft PowerPoint for Android
	Microsoft Edge for iOS
Windows Server 2025	Microsoft OneNote for Android
Windows Server 2022, 23H2 Edition (Server Core installation)	Microsoft PowerBI for iOS
	Microsoft PowerBI for Android
Windows 11 Version 24H2 for x64-based Systems	Microsoft 365 Copilot for Android
Windows 11 Version 24H2 for ARM64-based Systems	Microsoft Outlook for iOS
	Microsoft Loop for iOS
Windows Server 2019 (Server Core installation)	Microsoft Word for iOS
Windows Server 2019	Microsoft PowerPoint for iOS
Windows Server 2012 R2	Microsoft Word for Android
Windows Server 2012	Microsoft Excel for Android
Windows Server 2012 (Server Core installation)	Microsoft Teams for Android
Microsoft .NET Framework 3.5 AND 4.8.1	Microsoft Teams for iOS
Microsoft Office LTSC for Mac 2021	Microsoft 365 Copilot for iOS
Microsoft 365 Apps for Enterprise for 64-bit Systems	Microsoft Outlook for Android
Microsoft 365 Apps for Enterprise for 32-bit Systems	Microsoft Outlook for Mac
Microsoft Office 2019 for 64-bit editions	Microsoft OneNote for iOS
Microsoft Office 2019 for 32-bit editions	Azure MCP Server Tools 1.0.0 (npm)
Microsoft SQL Server 2019 for x64-based Systems (CU 32)	Azure MCP Server Tools 1.0.0 (NuGet)
	Azure MCP Server Tools 2.0.0 (PyPi)
Microsoft SQL Server 2022 for x64-based Systems (GDR)	Azure MCP Server Tools 2.0.0 (npm)
	Windows ADK for Windows 10, version 2004
Microsoft SQL Server 2017 for x64-based Systems (CU 31)	Windows ADK for Windows Server 2022
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 Azure Connect Feature Pack	Windows ADK for Windows 11, version 22H2
	Windows ADK for Windows 11, version 23H2
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR)	
Microsoft SQL Server 2019 for x64-based Systems (GDR)	Windows ADK for Windows 11, version 24H2
	Azure Automation Hybrid Worker Windows Extension
Microsoft Excel 2016 (64-bit edition)	
Microsoft Excel 2016 (32-bit edition)	ASP.NET Core 10.0
Microsoft Office LTSC for Mac 2024	ASP.NET Core 9.0
Microsoft Office LTSC 2024 for 64-bit editions	ASP.NET Core 8.0
Microsoft Office LTSC 2024 for 32-bit editions	Microsoft Authenticator for IOS
Microsoft Office LTSC 2021 for 32-bit editions	Microsoft Authenticator for Android
Office Online Server	Azure MCP Server Tools 2.0.0 (NuGet)
Microsoft SQL Server 2017 for x64-based Systems (GDR)	Arc Enabled Servers - Azure Connected Machine Agent
Microsoft SQL Server 2022 for x64-based Systems (CU 24)	Microsoft Office for Android
	Azure Linux Virtual Machines with Azure Diagnostics extension
Microsoft SQL Server 2025 for x64-based Systems (GDR)	
Microsoft SQL Server 2025 for x64-based Systems (CU3)	Azure IoT Explorer
	GitHub Repo: Zero Shot scFoundation
Azure Logic Apps	Microsoft Azure AD SSH Login extension for Linux
PowerShell 7.4	
PowerShell 7.5	Microsoft.Bcl.Memory 9.0
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2	Microsoft.Bcl.Memory 10.0
Microsoft .NET Framework 3.5	Microsoft SQL Server 2025 for x64-based Systems (CU2)
Microsoft Dynamics 365 (on-premises) version 9.0	
Microsoft Defender Antimalware Platform	Microsoft SQL Server 2022 for x64-based Systems (CU 23)
Azure Monitor Agent	
.NET 9.0 installed on Windows	System Center Operations Manager 2025
.NET 9.0 installed on Mac OS	System Center Operations Manager 2022
.NET 9.0 installed on Linux	System Center Operations Manager 2019
.NET 8.0 installed on Mac OS	Windows Admin Center in Azure Portal
.NET 8.0 installed on Linux	

Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Improper Neutralization of Escape, Meta, or Control Sequences Vulnerability (CVE-2025-55754)
Description	IBM has released a security update addressing a vulnerability that exists in their Storage Sentinel Product. **CVE-2025-55754**: Improper Neutralization of Escape, Meta, or Control Sequences vulnerability in Apache Tomcat. Tomcat did not escape ANSI escape sequences in log messages. If Tomcat was running in a console on a Windows operating system, and the console supported ANSI escape sequences, it was possible for an attacker to use a specially crafted URL to inject ANSI escape sequences to manipulate the console and the clipboard and attempt to trick an administrator into running an attacker controlled command. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Defender Copy Data Management – Versions 2.2.0.0 - 2.2.28.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7268262

Affected Product	**Synology**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47960, CVE-2021-47961)
Description	Synology has released a security update addressing multiple vulnerabilities that exist in their product. **CVE-2021-47960:** A files or directories accessible to external parties vulnerability allows remote attackers to access files within the installation directory via a local HTTP server bound to the loopback interface. By leveraging user interaction with a crafted web page, attackers may retrieve sensitive files such as configuration files, certificates, and logs, leading to information disclosure. **CVE-2021-47961:** A plaintext storage of a password vulnerability allows remote attackers to access or influence the user's PIN code due to insecure storage. This may lead to unauthorized VPN configuration and potential interception of subsequent VPN traffic when combined with user interaction. Synology advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Synology SSL VPN Client – Versions prior to 1.4.5-0684
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_26_05

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. SUSE 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.suse.com/support/update/

Affected Product	**Dell**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PowerEdge R6715, R7715, R6725, R7725, M7725, XE7745 - Versions prior to 1.6.4 PowerEdge R7725xd - Versions prior to 1.6.5 PowerEdge XE9785 - Versions prior to 1.1.4 PowerEdge XE9785L - Versions prior to 1.2.1 PowerEdge R6615, R7615, R6625, R7625, Dell XC Core XC7625 - Versions prior to 1.14.1, 1.16.2 PowerEdge C6615 - Versions prior to 1.9.1, 1.11.2 PowerEdge XE9685L - Versions prior to 1.3.4 PowerEdge R6515, R6525, R7515, R7525, C6525, Dell EMC XC Core XC7525 - Versions prior to 2.21.1, 2.23.1 PowerEdge XE8545 - Versions prior to 2.19.1, 2.21.0 DD OS 8.6 — Versions 7.7.1.0 through 8.6.0.0 DD OS 8.7 — Versions 7.7.1.0 through 8.7.0.0 DD OS 8.3.1 — Versions 8.3.1.0 through 8.3.1.20 DD OS 7.13.1 — Versions 7.13.1.0 through 7.13.1.60 DD OS 8.5 — Versions 8.3.0.0 through 8.5.0.0 PowerProtect DP Series Appliance (IDPA) — Versions prior to 2.7.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000452207/dsa-2026-004-security-update-for-dell-amd-based-poweredge-server-vulnerability • https://www.dell.com/support/kbdoc/en-us/000452216/dsa-2026-041-security-update-for-dell-amd-based-poweredge-server-vulnerability • https://www.dell.com/support/kbdoc/en-us/000452212/dsa-2026-043-security-update-for-dell-amd-based-poweredge-server-vulnerability • https://www.dell.com/support/kbdoc/en-us/000450699/dsa-2026-060-security-update-for-dell-powerprotect-data-domain-multiple-vulnerabilities

Affected Product	**AMD**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-54510, CVE-2025-54502, CVE-2023-20585)
Description	AMD has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-54510:** A missing lock verification in AMD Secure Processor (ASP) firmware may permit a locally authenticated attacker with administrative privileges to alter MMIO routing on some Zen 5-based products, potentially compromising guest system integrity. **CVE-2025-54502:** Incorrect use of boot service in the AMD Platform Configuration Blob (APCB) SMM driver could allow a privileged attacker with local access (Ring 0) to achieve privilege escalation potentially resulting in arbitrary code execution. **CVE-2023-20585:** Insufficient checks of the RMP on host buffer access in IOMMU may allow an attacker with privileges and a compromised hypervisor to trigger an out of bounds condition without RMP checks, resulting in a potential loss of confidential guest integrity. AMD advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	AMD EPYC™ Embedded 7002 Series Processors AMD EPYC™ Embedded 7003 Series Processors AMD EPYC™ Embedded 8004 Series Processors AMD EPYC™ Embedded 9004 Series Processors AMD EPYC™ Embedded 9005 Series Processors AMD EPYC™ 4004 Series Processors AMD EPYC™ 7002 Series Processors AMD EPYC™ 7003 Series Processors AMD EPYC™ 8004 Series Processors AMD EPYC™ 9004 Series Processors AMD EPYC™ 9005 Series Processors AMD EPYC™ 9V64H Processor AMD Instinct™ MI300A Series Processors
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7054.html https://www.amd.com/en/resources/product-security/bulletin/amd-sb-3034.html https://www.amd.com/en/resources/product-security/bulletin/amd-sb-3016.html

Affected Product	**Juniper Networks**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-30650, CVE-2022-24805)
Description	Juniper Networks has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-30650:** A Missing Authentication for Critical Function vulnerability in command processing of Juniper Networks Junos OS allows a privileged local attacker to gain access to Linux-based line cards as root. This issue affects systems running Junos OS using Linux-based line cards **CVE-2022-24805:** A buffer overflow in the handling of the `INDEX` of `NET-SNMP-VACM-MIB` can cause an out-of-bounds memory access. A user with read-only credentials can exploit the issue. Juniper Networks advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Junos OS: • All versions before 22.4R3-S8 • All versions before 23.2R2-S6, • 23.4 versions before 23.4R2-S7, • 24.2 versions before 24.2R2-S4, • 24.4 versions before 24.4R2-S3, • 25.2 versions before 25.2R1-S2, 25.2R2; • From 23.2 before 23.2R2-S6, • From 23.4 before 23.4R2-S6, • From 24.2 before 24.2R2-S3, • From 24.4 before 24.4R2, • From 25.2 before 25.2R2. Junos OS Evolved: • All versions before 23.2R2-S6-EVO, • 23.4 versions before 23.4R2-S8-EVO, • 24.2 versions before 24.2R2-S4-EVO, • 24.4 versions before 24.4R2-S3-EVO, • 25.2 versions before 25.2R1-S2-EVO, 25.2R2-EVO. Junos OS using Linux-based line cards: • MPC7, MPC8, MPC9, MPC10, MPC11 • LC2101, LC2103 • LC480, LC4800, LC9600 • MX304 (built-in FPC) • MX-SPC3 • SRX5K-SPC3 • EX9200-40XS • FPC3-PTX-U2, FPC3-PTX-U3 • FPC3-SFF-PTX • LC1101, LC1102, LC1104, LC1105
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-Privileged-local-user-can-gain-access-to-a-Linux-based-FPC-as-root-CVE-2025-30650 • https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-CVE-2022-24805-resolved-in-net-SNMP

Affected Product	**Fortinet**
Severity	**High,** **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-40688, CVE-2026-25691, CVE-2026-27316, CVE-2026-39810, CVE-2026-39811, CVE-2025-53847, CVE-2026-39814, CVE-2026-39809, CVE-2026-39812, CVE-2025-61624, CVE-2025-68649, CVE-2025-61886, CVE-2026-39815, CVE-2025-61848, CVE-2024-23104)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise 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/advisory

Affected Product	**HPE**
Severity	**High,** **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-22885, CVE-2025-54510, CVE-2025-54502, CVE-2025-50585)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their product. These vulnerabilities could be exploited by malicious users to compromise affected systems. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE ProLiant DL325, DL345, DL365, DL385 Gen11 Server - Prior to 2.70_08-07-2025, 3.00_02-06-2026 HPE ProLiant DL145 Gen11 - Prior to 1.70_08-07-2025, 1.80_02-06-2026 HPE ProLiant DL325, DL385 Gen10 Plus, DL325, DL385 Gen10 Plus v2, DL345, DL365 Gen10 Plus server - Prior to 3.90_10-03-2025, 4.00_01-09-2026 HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to 3.90_10-03-2025, 4.00_01-09-2026 HPE ProLiant Compute DL325, DL345 Gen12 - Prior to 1.40_01-09-2026 HPE ProLiant DL325, DL385 Gen10 Server - Prior to 3.70_01-09-2026 HPE SimpliVity 380 Gen11 - Prior to SimpliVity Gen11 Support Pack v2026_0318
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05015en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05035en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05034en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05036en_us&docLocale=en_US

Affected Product	**IBM**
Severity	**High,** **Medium,** **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Storage Defender Copy Data Management – Versions 2.2.0.0 - 2.2.28.1 IBM Storage Sentinel Anomaly Scan Engine – Versions 1.1.0 - 1.1.12 IBM WebSphere Remote Server – Versions 8.5, 9.0, 9.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7268262 https://www.ibm.com/support/pages/node/7268263 https://www.ibm.com/support/pages/node/7268264 https://www.ibm.com/support/pages/node/7268265 https://www.ibm.com/support/pages/node/7268926 https://www.ibm.com/support/pages/node/7269156

Affected Product	**SAP**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-34256, CVE-2025-64775, CVE-2026-34264, CVE-2026-34261, CVE-2026-27677, CVE-2026-27678, CVE-2026-27679, CVE-2026-0512, CVE-2026-27674, CVE-2026-34257, CVE-2026-34262, CVE-2026-27673, CVE-2026-27672, CVE-2026-27676, CVE-2025-42899, CVE-2026-24318, CVE-2026-27683, CVE-2026-27680, CVE-2026-27675)
Description	SAP has released security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. SAP advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SAP ERP and SAP S/4 HANA (Private Cloud and On-Premise) • SAP_FIN 618, 720, 730 • EA-FIN 617, 700 • SAPSCORE 135 • S4CORE 102, 103, 104, 105, 106, 107, 108, 109 • EA-APPL 600, 602, 603, 604, 605, 606 SAP BusinessObjects Business Intelligence Platform • ENTERPRISE 430, 2025, 2027 SAP Human Capital Management for SAP S/4HANA • S4HCMRXX 100, 101, 102 • SAP_HRRXX 600, 604, 608 SAP Business Analytics and SAP Content Management • S4HCMRXX 100, 101, 102 • SAP_HRRXX 600, 604, 608 SAP S/4HANA OData Service (Manage Reference Equipment) • S4CORE 109 SAP S/4HANA Backend OData Service (Manage Reference Structures) • S4CORE 109 SAP S/4HANA Frontend OData Service (Manage Reference Structures) • UIS4H 109 SAP Supplier Relationship Management (SICF Handler in SRM Catalog) • SRM_SERVER 702, 713, 714 SAP NetWeaver Application Server Java (Web Dynpro Java) • WD-RUNTIME 7.50 SAP NetWeaver Application Server ABAP • SAP_BASIS 700, 701, 702, 731, 740, 750, 752, 753, 754, 755, 756, 757, 758, 816 SAP HANA Cockpit and HANA Database Explorer • SAP_HANA_COCKPIT 2.0 SAP S/4HANA (Private Cloud and On-Premise) • S4CORE 105, 106, 107, 108, 109 • FI-CA 606, 616, 617, 618 Material Master Application • S4CORE 102, 103, 104, 105, 106, 107, 108, 109 • SCM_BASIS 700, 701, 702, 712, 713, 714 SAP S/4HANA OData Service (Manage Technical Object Structures) • S4CORE 109 SAP S4CORE (Manage Journal Entries) • S4CORE 104, 105, 106, 107, 108 SAP BusinessObjects Business Intelligence Platform (Session Management / XSS) • ENTERPRISE 430, 2025, 2027 SAP NetWeaver Application Server ABAP (SAP_UI CSS Injection) • SAP_UI 758, 816 SAP Landscape Transformation • DMIS 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752, 2020 • S4CORE 102, 103, 104, 105, 106, 107, 108, 109
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2026.html

Affected Product	**Apache Tomcat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-34483, CVE-2026-34486, CVE-2026-34487, CVE-2026-34500)
Description	Apache Tomcat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Apache Tomcat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Apache Tomcat – Versions 11.0.0-M14 to 11.0.20 Apache Tomcat – Versions 11.0.0-M1 to 11.0.20 Apache Tomcat – Versions 10.1.22 to 10.1.53 Apache Tomcat – Versions 10.1.0-M1 to 10.1.53 Apache Tomcat – Versions 9.0.13 to 9.0.116
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.21 https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.54 https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.117

Affected Product	**NetApp**
Severity	**Medium**
Affected Vulnerability	Improper Certificate Validation Vulnerability (CVE-2025-61727)
Description	NetApp has released a security update addressing a vulnerability that exists in their product. **CVE-2025-61727:** Golang versions prior to 1.24.11 and 1.25 prior to 1.25.5 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, or addition or modification of data. NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Trident & Trident Protect
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20260130-0003

Affected Product	**Ivanti**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-4913, CVE-2026-4914)
Description	Ivanti has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-4913:** Improper protection of an alternate path in Ivanti N-ITSM before version 2025.4 allows a remote authenticated attacker to retain access when their account has been disabled. **CVE-2026-4914:** Stored XSS in Ivanti N-ITSM before version 2025.4 allows a remote authenticated attacker to obtain limited information from other user sessions. User interaction is required. Ivanti advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ivanti Neurons for ITSM (On-Premise) – Version 2025.3 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Neurons-for-ITSM-CVE-2026-4913-CVE-2026-4914?language=en_US

Affected Product	**F5**
Severity	**Low**
Affected Vulnerability	Use After Free Vulnerability (CVE-2025-10911)
Description	F5 has released a security update addressing a vulnerability that exists in their products. **CVE-2025-10911**: A use-after-free vulnerability was found in libxslt while parsing xsl nodes that may lead to the dereference of expired pointers and application crash. F5 advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	F5OS-A 1.x • Versions 1.8.0 - 1.8.3 • Versions 1.5.1 - 1.5.4 F5OS-C 1.x • Versions 1.8.0 - 1.8.2 • Versions 1.6.0 - 1.6.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000160723

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.