Advisory Alert

Alert Number: AAA20250115 **Date:** January 15, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SAP	**Critical**	Multiple Vulnerabilities
FortiGuard	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
Ivanti	**Critical**	Multiple Sensitive Information Disclosure Vulnerabilities
IBM	**Critical**	Cross-Site Scripting Vulnerability
Juniper	**High**	Multiple Vulnerabilities
Veeam	**High**	Server-Side Request Forgery Vulnerability
Ivanti	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
SAP	**High**, **Medium**, **Low**	Multiple Vulnerabilities
FortiGuard	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-0070, CVE-2025-0066)
Description	SAP has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-0070 -** SAP NetWeaver Application Server for ABAP and ABAP Platform allows an authenticated attacker to obtain illegitimate access to the system by exploiting improper authentication checks, resulting in privilege escalation. On successful exploitation, this can result in potential security concerns. This results in a high impact on confidentiality, integrity, and availability. **CVE-2025-0066 -** Under certain conditions SAP NetWeaver AS for ABAP and ABAP Platform (Internet Communication Framework) allows an attacker to access restricted information due to weak access controls. This can have a significant impact on the confidentiality, integrity, and availability of an application SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SAP NetWeaver Application Server for ABAP and ABAP Platform Versions - KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, 8.04, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 7.97, 8.04, 9.12, 9.13, 9.14 SAP NetWeaver AS for ABAP and ABAP Platform (Internet Communication Framework) Versions - SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 912, SAP_BASIS 913, SAP_BASIS 914
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/january-2025.html

Affected Product	**FortiGuard**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-55591, CVE-2023-37936)
Description	FortiGuard has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-55591 -** An Authentication Bypass Using an Alternate Path or Channel vulnerability affecting FortiOS and FortiProxy may allow a remote attacker to gain super-admin privileges via crafted requests to Node.js websocket module. **CVE-2023-37936 -** A use of hard-coded cryptographic key vulnerability in FortiSwitch may allow a remote unauthenticated attacker in posession of the key to execute unauthorized code via crafted cryptographic requests. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiOS 7.0 - 7.0.0 through 7.0.16 FortiProxy 7.2 - 7.2.0 through 7.2.12 FortiProxy 7.0 - 7.0.0 through 7.0.19 FortiSwitch 7.4 - 7.4.0 FortiSwitch 7.2 - 7.2.0 through 7.2.5 FortiSwitch 7.0 - 7.0.0 through 7.0.7 FortiSwitch 6.4 - 6.4.0 through 6.4.13 FortiSwitch 6.2 - 6.2.0 through 6.2.7 FortiSwitch 6.0 - 6.0.0 through 6.0.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.fortiguard.com/psirt/FG-IR-24-535 • https://www.fortiguard.com/psirt/FG-IR-23-260

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38138, CVE-2024-38186, CVE-2024-38158, CVE-2024-38157, CVE-2024-38155, CVE-2024-38152, CVE-2024-38146, CVE-2024-38143, CVE-2024-38140, CVE-2024-38134, CVE-2024-38127, CVE-2024-38122, CVE-2024-38117, CVE-2024-38114, CVE-2024-38106, CVE-2024-38199, CVE-2024-38193, CVE-2024-38178, CVE-2024-37968, CVE-2024-38109, CVE-2024-38223, CVE-2024-38215, CVE-2024-38214, CVE-2024-38120, CVE-2024-38211, CVE-2022-3775, CVE-2024-38163, CVE-2024-38195, CVE-2024-38189, CVE-2024-38187, CVE-2024-38185, CVE-2024-38180, CVE-2024-38177, CVE-2024-38173, CVE-2024-38171, CVE-2024-38170, CVE-2024-38169, CVE-2024-38165, CVE-2024-38162, CVE-2024-38154, CVE-2024-38153, CVE-2024-38151, CVE-2024-38150, CVE-2024-38148, CVE-2024-38147, CVE-2024-38145, CVE-2024-38144, CVE-2024-38142, CVE-2024-38141, CVE-2024-38137, CVE-2024-38136, CVE-2024-38135, CVE-2024-38133, CVE-2024-38132, CVE-2024-38131, CVE-2024-38130, CVE-2024-38128, CVE-2024-38126, CVE-2024-38125, CVE-2024-38121, CVE-2024-38118, CVE-2024-38116, CVE-2024-38115, CVE-2024-29995, CVE-2024-38107, CVE-2024-38098, CVE-2024-38063, CVE-2024-38084, CVE-2023-40547, CVE-2024-38213, CVE-2024-38201, CVE-2024-38198, CVE-2024-38197, CVE-2024-38196, CVE-2024-38191, CVE-2024-38184, CVE-2024-38172, CVE-2024-38168, CVE-2024-38167, CVE-2024-38161, CVE-2024-38160, CVE-2024-38159, CVE-2024-38123, CVE-2024-38108, CVE-2022-2601, CVE-2024-7536, CVE-2024-7535, CVE-2024-7534, CVE-2024-7533, CVE-2024-7532, CVE-2024-7550, CVE-2024-38200, CVE-2024-38219, CVE-2024-38218, CVE-2024-38202, CVE-2024-21302, CVE-2024-38206, CVE-2024-38166, CVE-2024-7256, CVE-2024-7255, CVE-2024-6990)
Description	Microsoft has issued the security update for the month of January addressing multiple vulnerabilities that exists in variety of Microsoft products, features, and roles. Updates include defense-in-depth updates to help strengthen security-related aspects, in addition to security improvements for the vulnerabilities. Microsoft advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	.NET 8.0 App Installer Azure Connected Machine Agent Azure CycleCloud 8.0.0 - 8.6.2 Azure Health Bot Azure IoT Hub Device Client SDK Azure Linux 3.0 ARM Azure Linux 3.0 x64 Azure Stack Hub C SDK for Azure IoT CBL Mariner 1.0 ARM CBL Mariner 1.0 x64 CBL Mariner 2.0 ARM CBL Mariner 2.0 x64 Dynamics CRM Service Portal Web Resource Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft Copilot Studio Microsoft Dynamics 365 (on-premises) version 9.1 Microsoft Edge (Chromium-based) Microsoft Office 2016 (32-bit edition) Microsoft Office 2016 (64-bit edition) Microsoft Office 2019 for 32-bit editions Microsoft Office 2019 for 64-bit editions Microsoft Office LTSC 2021 for 32-bit editions Microsoft Office LTSC 2021 for 64-bit editions Microsoft Office LTSC for Mac 2021 Microsoft OfficePLUS Microsoft Outlook 2016 (32-bit edition) Microsoft Outlook 2016 (64-bit edition) Microsoft PowerPoint 2016 (32-bit edition) Microsoft PowerPoint 2016 (64-bit edition) Microsoft Project 2016 (32-bit edition) Microsoft Project 2016 (64-bit edition) Microsoft Teams for iOS Microsoft Visual Studio 2022 version 17.10, version 17.6, version 17.8 Remote Desktop client for Windows Desktop Windows 10 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 21H2 for 32-bit Systems	Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows 11 Version 24H2 for x64-based Systems Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2012 Windows Server 2012 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation) Windows Server 2016 Windows Server 2016 (Server Core installation) Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server 2022 Windows Server 2022 (Server Core installation) Windows Server 2022, 23H2 Edition (Server Core installation)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2025-Jan

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Multiple Sensitive Information Disclosure Vulnerabilities (CVE-2024-10811, CVE-2024-13161, CVE-2024-13160, CVE-2024-13159)
Description	Ivanti has released security updates addressing Sensitive Information Disclosure Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Endpoint Manager Version - 2024 November security update and prior, 2022 SU6 November security update and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6?language=en_US

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Cross-Site Scripting Vulnerability (CVE-2024-47875)
Description	IBM has release security updates addressing a Cross-Site Scripting Vulnerability that exist in their products. **CVE-2024-47875 -** DOMPurify is a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTML, MathML and SVG. DOMpurify was vulnerable to nesting-based mXSS. This vulnerability is fixed in 2.5.0 and 3.1.3. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QRadar Log Source Management App Version - 1.0.0 - 7.0.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7180725

Affected Product	**Juniper**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-6387, CVE-2024-39894)
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-6387 -** A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. **CVE-2024-39894 -** OpenSSH 9.5 through 9.7 before 9.8 sometimes allows timing attacks against echo-off password entry (e.g., for su and Sudo) because of an ObscureKeystrokeTiming logic error. Similarly, other timing attacks against keystroke entry could occur. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Junos OS Evolved 24.2-EVO before 24.2R1-S2-EVO, 24.2R2-EVO
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://supportportal.juniper.net/s/article/2025-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Multiple-vulnerabilities-resolved-in-OpenSSH?language=en_US

Affected Product	**Veeam**
Severity	**High**
Affected Vulnerability	Server-Side Request Forgery Vulnerability (CVE-2025-23082)
Description	Veeam has released security updates to address a Server-Side Request Forgery Vulnerability that exist in their products. **CVE-2025-23082 -** This vulnerability that may allow an attacker to utilize Server-Side Request Forgery (SSRF) to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Backup for Microsoft Azure 7.1.0.22
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4709

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-13158, CVE-2024-13162, CVE-2024-13163, CVE-2024-13164, CVE-2024-13165, CVE-2024-13166, CVE-2024-13167, CVE-2024-13168, CVE-2024-13169, CVE-2024-13170, CVE-2024-13171, CVE-2024-13172, CVE-2024-13179, CVE-2024-13180, CVE-2024-13181, CVE-2024-10630)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Remote Code Execution, Denial of Service, Escalate their Privileges, Bypass Authentication. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Endpoint Manager Version - 2024 November security update and prior, 2022 SU6 November security update and prior Ivanti Avalanche Version - 6.4.6 and prior Ivanti Application Control Version - 2024.3 and prior, 2024.1 and prior, 2023.3 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6?language=en_US • https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-7-Multiple-CVEs?language=en_US • https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Application-Control-Engine-CVE-2024-10630?language=en_US

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 cause Use-after-free, Integer Overflow, Memory Corruption, Memory Leak, Denial of Service. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.4, 15.3 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP3 SUSE Linux Enterprise Live Patching 15-SP3 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Server 15 SP3 SUSE Linux Enterprise Server for SAP Applications 15 SP3 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 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/2025/suse-su-20250109-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250108-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250107-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250106-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250105-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250103-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250101-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250100-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250098-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250097-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250094-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250091-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250090-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250089-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250083-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250085-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250084-1/

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-43796, CVE-2024-45590, CVE-2024-55565, CVE-2024-45801, CVE-2024-21538, CVE-2024-48948, CVE-2024-4068, CVE-2024-47068, CVE-2024-43788, CVE-2024-4067, CVE-2024-43800, CVE-2024-45296, CVE-2024-37890, CVE-2024-33883, CVE-2024-52798, CVE-2024-43799, CVE-2024-21536, CVE-2024-42461, CVE-2024-42460, CVE-2024-42459, CVE-2024-48949, CVE-2024-47764, CVE-2021-29825, CVE-2024-20932, CVE-2024-20952, CVE-2024-20918, CVE-2024-20921, CVE-2024-20926, CVE-2024-20945, CVE-2024-22361, CVE-2023-22081, CVE-2023-22067, CVE-2023-4807, CVE-2023-5676)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Server Crash, Information Disclosure, Cross-Site Scripting, Denial of Service, IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QRadar Log Source Management App Version - 1.0.0 - 7.0.10 IBM Db2 Version - 10.5.0 - 10.5.11, 11.1.4 - 11.1.4.7, 11.5.0 - 11.5.6 Db2 Query Management Facility Version - 13.1.2, 13.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7180725 • https://www.ibm.com/support/pages/node/6489499 • https://www.ibm.com/support/pages/node/7180894 • https://www.ibm.com/support/pages/node/7180895

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-0063, CVE-2025-0061, CVE-2025-0069, CVE-2025-0058, CVE-2025-0067, CVE-2025-0055, CVE-2025-0056, CVE-2025-0059, CVE-2025-0053, CVE-2025-0057, CVE-2025-0068, CVE-2024-29131, CVE-2024-29133)
Description	SAP has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause SQL Injection, Information Disclosure, Cross-Site Scripting, Buffer overflow, SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SAP NetWeaver AS ABAP and ABAP Platform, Version - SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758 SAP BusinessObjects Business Intelligence Platform, Versions - ENTERPRISE 420, 430, 2025 SAPSetup, Version - LMSAPSETUP 9.0 SAP Business Workflow and SAP Flexible Workflow, Version - SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 912, SAP_BASIS 913, SAP_BASIS 914 SAP NetWeaver Application Server Java, Version - WD-RUNTIME 7.50 SAP GUI for Windows, Versions - BC-FES-GUI 8.0 SAP GUI for Java, Versions - BC-FES-JAV 7.80 SAP NetWeaver Application Server ABAP (applications based on SAP GUI for HTML), Versions - KRNL64UC 7.53, KERNEL 7.53, 7.54, 7.77, 7.89, 7.93, 9.12, 9.14 SAP NetWeaver Application Server for ABAP and ABAP Platform, Version - SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757 SAP NetWeaver AS JAVA (User Admin Application), Version - ENGINEAPI 7.50, SERVERCORE 7.50, UMEADMIN 7.50 SAP NetWeaver Application Server ABAP, Versions - SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758 SAP BusinessObjects Business Intelligence Platform (Crystal Reports for Enterprise), Version - ENTERPRISE 430
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/january-2025.html

Affected Product	**FortiGuard**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-23439, CVE-2024-35280, CVE-2024-48886, CVE-2024-50563, CVE-2024-36510, CVE-2024-46666, CVE-2024-48893, CVE-2024-35276, CVE-2024-36504, CVE-2024-35275, CVE-2024-35278, CVE-2023-37937, CVE-2024-56497, CVE-2024-3596, CVE-2024-46664, CVE-2024-47566, CVE-2024-48884, CVE-2024-48885, CVE-2024-35273, CVE-2024-52963, CVE-2024-46670, CVE-2024-48890, CVE-2024-27778, CVE-2024-50566, CVE-2023-42785, CVE-2023-42786, CVE-2024-33503, CVE-2024-45331, CVE-2024-46668, CVE-2024-46669, CVE-2024-46669, CVE-2024-36506,CVE-2024-33502, CVE-2024-45326, CVE-2024-47573, CVE-2024-47572, CVE-2023-46715, CVE-2023-37936, CVE-2024-50564, CVE-2024-52967, CVE-2024-21758, CVE-2024-26012,CVE-2024-32115, CVE-2024-47571, CVE-2024-54021, CVE-2024-46665, CVE-2024-23106, CVE-2024-46667, CVE-2024-46662, CVE-2023-4863, CVE-2024-52969, CVE-2024-55591, CVE-2024-36512, CVE-2024-32115)
Description	FortiGuard has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20342, CVE-2025-20126)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-20342 -** This vulnerability is due to an incorrect connection count comparison. An attacker could exploit this vulnerability by sending traffic through an affected device at a rate that exceeds a configured rate filter. A successful exploit could allow the attacker to successfully bypass the rate filter. This could allow unintended traffic to enter the network protected by the affected device. **CVE-2024-50570** - This vulnerability exists because the affected software does not properly validate certificates for hosted metrics services. An on-path attacker could exploit this vulnerability by intercepting network traffic using a crafted certificate. A successful exploit could allow the attacker to masquerade as a trusted host and monitor or change communications between the remote metrics service and the vulnerable client. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco FTD Software Release 7.0 and earlier, 7.1 - 7.4 Cisco ThousandEyes Agent - macOS1.206.3, RoomOS 1.207.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-rf-bypass-OY8f3pnM • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-thousandeyes-cert-pqtJUv9N

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.