Advisory Alert

Alert Number: AAA20241009 **Date:** October 9, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**Critical**	Remote Code Execution Vulnerability
Ivanti	**Critical**	Improper Input Validation Vulnerability
SAP	**Critical**	Improper Authentication Vulnerability
Synology	**Critical**	Authentication Bypass Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
HPE	**High**	Information Disclosure Vulnerability
Ivanti	**High, Medium**	Multiple Vulnerabilities
SAP	**High, Medium**	Multiple Vulnerabilities
IBM	**Medium**	Stored Cross-Site Scripting Vulnerability
Fortiguard	**Medium, Low**	Multiple Vulnerabilities
Intel	**Low**	Information Disclosure Vulnerability

Description

Affected Product	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2024-47561)
Description	Red Hat has released security updates addressing a Remote Code Execution vulnerability in Apache Avro that affects their products. **CVE-2024-47561-** A vulnerability was found in Apache Avro. The project is affected and at risk if it accepts an org.apache.Avro/avroAvro schema for parsing provided by an end user. This flaw allows an attacker to trigger remote code execution by using the special "java-class" attribute. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 7.4 for RHEL 9 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 8 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 7 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:7812 • https://access.redhat.com/errata/RHSA-2024:7811

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Improper Input Validation Vulnerability (CVE-2024-37404)
Description	Ivanti has released security updates addressing an Improper Input Validation Vulnerability that exists in their products. **CVE-2024-37404 -** An Improper Input Validation Vulnerability in the admin portal of Ivanti Connect Secure before 22.7R2.1 and 9.1R18.9, or Ivanti Policy Secure before 22.7R1.1 allows a remote authenticated attacker to achieve remote code execution. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Connect Secure All version before 22.7R2.1 Ivanti Policy Secure All versions before 22.7R1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-and-Policy-Secure-CVE-2024-37404?language=en_US

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Improper Authentication Vulnerability (CVE-2024-41730)
Description	SAP has issued security updates addressing an Improper Authentication Vulnerability that exists in their products **CVE-2024-41730 -** In SAP BusinessObjects Business Intelligence Platform, if Single Signed On is enabled on Enterprise authentication, an unauthorized user can get a logon token using a REST endpoint. The attacker can fully compromise the system resulting in High impact on confidentiality, integrity and availability. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SAP BusinessObjects Business Intelligence Platform, Versions - ENTERPRISE 420 ,430, 440
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/october-2024.html

Affected Product	**Synology**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2024-45409)
Description	Synology has issued security updates addressing an Authentication Bypass that exists in their products. **CVE-2024-45409 -** The Ruby SAML library is for implementing the client side of a SAML authorization. Ruby-SAML in <= 12.2 and 1.13.0 <= 1.16.0 does not properly verify the signature of the SAML Response. An unauthenticated attacker with access to any signed saml document (by the IdP) can thus forge a SAML Response/Assertion with arbitrary contents. This would allow the attacker to log in as arbitrary user within the vulnerable system Synology advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	GtiLab for DSM 6.2 below version 13.12.2-0074
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_24_12

Affected Product	**Microsoft**	
Severity	**Critical**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-43484, CVE-2024-43483, CVE-2024-43488, CVE-2024-43611, CVE-2024-43593, CVE-2024-43582, CVE-2024-43570, CVE-2024-43562, CVE-2024-43558, CVE-2024-43553, CVE-2024-43549, CVE-2024-43547, CVE-2024-43536, CVE-2024-43520, CVE-2024-43511, CVE-2024-43468, CVE-2024-43497, CVE-2024-43485, CVE-2024-43453, CVE-2024-38262, CVE-2024-37983, CVE-2024-43607, CVE-2024-43573, CVE-2024-43540, CVE-2024-43534, CVE-2024-43526, CVE-2024-43518, CVE-2024-43506, CVE-2024-43614, CVE-2024-43583, CVE-2024-43603, CVE-2024-43599, CVE-2024-43592, CVE-2024-43591, CVE-2024-43590, CVE-2024-43589, CVE-2024-43585, CVE-2024-43584, CVE-2024-43575, CVE-2024-43574, CVE-2024-43572, CVE-2024-43571, CVE-2024-43567)	
Description	Microsoft has released a monthly security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Remote Code Execution, Web Security Feature Bypass, Information Disclosure. Microsoft advises to apply security fixes at your earliest to protect systems from potential threats.	
Affected Products	Microsoft .NET Framework 3.5 AND 4.8.1 Microsoft .NET Framework 4.8 Visual Studio Code Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems 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 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows Server 2016 Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 for 32-bit Systems Windows 11 Version 24H2 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 Server 2022, 23H2 Edition (Server Core installation) Windows Server 2022 (Server Core installation) Windows Server 2022 Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 11 Version 24H2 for ARM64-based Systems Microsoft Configuration Manager 2403 Microsoft Configuration Manager 2309 Microsoft Configuration Manager 2303 DeepSpeed .NET 8.0 installed on Windows .NET 6.0 installed on Mac OS Windows 11 Version 23H2 for x64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Microsoft .NET Framework 3.5 AND 4.8 Microsoft .NET Framework 3.5.1 Microsoft .NET Framework 3.5 Microsoft .NET Framework 3.0 Service Pack 2	Microsoft .NET Framework 2.0 Service Pack 2 Microsoft .NET Framework 4.6/4.6.2 Microsoft .NET Framework 4.6.2 Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 Microsoft .NET Framework 3.5 AND 4.7.2 Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2016 (Server Core installation) Microsoft Defender for Endpoint for Linux Windows 11 Version 23H2 for ARM64-based Systems Microsoft Visual Studio 2015 Update 3 Microsoft Visual Studio 2022 version 17.10 Microsoft Visual Studio 2022 version 17.8 Microsoft Visual Studio 2022 version 17.6 Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10) Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8) Microsoft Visual Studio 2022 version 17.11 Azure Service Connector Azure CLI Visual C++ Redistributable Installer .NET 8.0 installed on Mac OS .NET 6.0 installed on Windows .NET 6.0 installed on Linux .NET 8.0 installed on Linux Microsoft Office LTSC 2024 for 64-bit editions Microsoft Office LTSC 2024 for 32-bit editions Microsoft Office LTSC 2021 for 32-bit editions Microsoft Office LTSC 2021 for 64-bit editions Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft Office 2019 for 64-bit editions Microsoft Office 2019 for 32-bit editions Power BI Report Server - May 2024 Microsoft Office 2016 (64-bit edition) Microsoft Office 2016 (32-bit edition) Microsoft Outlook for Android CBL Mariner 2.0 x64 CBL Mariner 2.0 ARM Remote Desktop client for Windows Desktop Microsoft Excel 2016 (64-bit edition) Microsoft Excel 2016 (32-bit edition) Microsoft SharePoint Server Subscription Edition Microsoft SharePoint Server 2019 Microsoft SharePoint Enterprise Server 2016 Azure Service Fabric 10.1 for Linux Azure Service Fabric 10.0 for Linux Azure Service Fabric 9.1 for Linux Azure Stack HCI 23H2 Azure Stack HCI 22H2 Azure Monitor Agent Microsoft Edge (Chromium-based)
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2024-Oct	

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2024-27457)
Description	HPE has released security updates addressing an information disclosure vulnerability that exists in Intel processors, which affects their products. **CVE-2024-27457** - Information disclosure vulnerability in Intel TDX Module firmware. An improper check for unusual or exceptional conditions in versions before 1.5.06 may allow a privileged user to potentially enable information disclosure via local access. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Alletra 4140 - Prior to v2.32_09-09-2024 HPE ProLiant DL110 Gen11 - Prior to v2.32_09-09-2024 HPE ProLiant DL320 Gen11 Server - Prior to v2.32_09-09-2024 HPE ProLiant DL360 Gen11 Server - Prior to v2.32_09-09-2024 HPE ProLiant DL380 Gen11 Server - Prior to v2.32_09-09-2024 HPE ProLiant DL380a Gen11 - Prior to v2.32_09-09-2024 HPE ProLiant ML110 Gen11 - Prior to v2.32_09-09-2024 HPE ProLiant ML350 Gen11 Server - Prior to v2.32_09-09-2024 HPE ProLiant DL560 Gen11 - Prior to v2.32_09-09-2024 HPE Synergy 480 Gen11 Compute Module - Prior to v2.32_09-09-2024 HPE Compute Edge Server e930t - Prior to v2.32_09-09-2024
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04710en_us&docLocale=en_US

Affected Product	**Ivanti**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-9379, CVE-2024-9380, CVE-2024-938, CVE-2024-7612, CVE-2024-9167, CVE-2024-47007, CVE-2024-47008, CVE-2024-47009, CVE-2024-47010, CVE-2024-47011)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause sensitive Information Disclosure, Denial of service, Authentication Bypass, Local Privilege Escalation Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti CSA (Cloud Services Appliance Versions 5.0.1 and prior Ivanti EPMM (Core) Versions 12.1.0.3 and prior Ivanti Velocity License Server Versions 5.1 versions prior to 5.1.2 Ivanti Avalanche 6.4.2.313 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-Cloud-Services-Appliance-CVE-2024-9379-CVE-2024-9380-CVE-2024-9381?language=en_US • https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2024-7612?language=en_US • https://forums.ivanti.com/s/article/Security-Advisory-Velocity-License-Server-CVE-2024-9167?language=en_US • https://forums.ivanti.com/s/article/Ivanti-Avalanche-6-4-5-Security-Advisory?language=en_US

Affected Product	**SAP**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0215, CVE-2022-0778, CVE-2023-0286, CVE-2022-23302, CVE-2024-22259, CVE-2024-38809, CVE-2024-38808, CVE-2024-37179, CVE-2024-39592, CVE-2024-45283, CVE-2024-45278, CVE-2024-47594, CVE-2024-45277, CVE-2024-45282, CVE-2024-41729, CVE-2024-42373, CVE-2024-37180)
Description	SAP has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Information Disclosure, Cross-Site Scripting, Use-after-free SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP Enterprise Project Connection, Version - 3.0 • SAP BusinessObjects Business Intelligence Platform (Web Intelligence), Version - ENTERPRISE 420, 430, 2025, ENTERPRISECLIENTTOOLS 420, 430, 2025 • SAP PDCE, Versions - S4CORE 102, 103, S4COREOP 104, 105, 106, 107, 108 • SAP NetWeaver AS for Java (Destination Service), Versions - 7.50 • SAP Commerce Backoffice, Versions - HY_COM 2205, COM_CLOUD 2211 • SAP NetWeaver Enterprise Portal (KMC), Version - KMC-BC 7.5 • SAP HANA Client, Version - HDB_CLIENT 2.0 • SAP S/4 HANA (Manage Bank Statements), Versions – S4CORE, 102, 103, 104, 105, 106, 107 • SAP NetWeaver BW (BEx Analyzer), Versions – DW4CORE 200, DW4CORE 300, DW4CORE 400, SAP_BW 700, SAP_BW 701, SAP_BW 702, SAP_BW 731, SAP_BW 740, SAP_BW 750, SAP_BW 751, SAP_BW 752, SAP_BW 753, SAP_BW 754, SAP_BW 755, SAP_BW 756, SAP_BW 757, SAP_BW 758 • SAP Student Life Cycle Management (SLcM), Versions – IS-PS-CA 617, 618, 802, 803, 804, 805, 806, 807, 808 • SAP NetWeaver Application Server for ABAP and ABAP Platform, 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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/october-2024.html

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Stored Cross-Site Scripting Vulnerability (CVE-2024-45073)
Description	IBM has issued security updates addressing a Stored Cross-Site Scripting that exists in their products. **CVE-2024-45073**- IBM WebSphere Application Server is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Remote Server Versions 9.1, 9.0, 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7172583

Affected Product	**Fortiguard**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45330, CVE-2024-33506, CVE-2024-26010)
Description	Fortiguard has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-45330 -** A use of externally-controlled format string vulnerability in FortiAnalyzer fazsvcd daemon may allow a remote privileged attacker with admin profile to execute arbitrary code or commands via specially crafted requests. **CVE-2024-33506 -** An exposure of sensitive information to an unauthorized actor vulnerability in FortiManager Administrative Domain (ADOM) may allow a remote authenticated attacker assigned to an ADOM to access device summary of other ADOMs via crafted HTTP requests. **CVE-2024-26010-** A stack-based overflow vulnerability [CWE-124] in FortiOS, FortiProxy, FortiPAM and FortiSwitchManager may allow a remote attacker to execute arbitrary code or command via crafted packets reaching the fgfmd daemon, under certain conditions which are outside the control of the attacker. Fortiguard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiAnalyzer Versions 7.2.2 through 7.2.5 FortiAnalyzer Versions 7.4.0 through 7.4.3 FortiAnalyzer Cloud Versions 7.2.2 through 7.2.6 FortiAnalyzer Cloud Versions 7.4.1 through 7.4.3 FortiManager Versions 7.0 all versions FortiManager Versions 7.2.0 through 7.2.5 FortiManager Versions 7.4.0 through 7.4.2 FortiOS 6.0 all versions FortiOS 6.2 all versions FortiOS 6.4 all versions FortiOS Versions 7.0.0 through 7.0.14 FortiOS Versions 7.2.0 through 7.2.7 FortiOS Versions 7.4.0 through 7.4.3 FortiPAM 1.0 all versions FortiPAM 1.1 all versions FortiPAM 1.2 all versions FortiProxy 1.0 all versions FortiProxy 1.1 all versions FortiProxy 1.2 all versions FortiProxy 2.0 all versions FortiProxy Versions 7.0.0 through 7.0.16 FortiProxy Versions 7.2.0 through 7.2.9 FortiProxy Versions 7.4.0 through 7.4.3 FortiSwitchManager Versions 7.0.1 through 7.0.3 FortiSwitchManager Versions 7.2.0 through 7.2.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.fortiguard.com/psirt/FG-IR-24-196 • https://www.fortiguard.com/psirt/FG-IR-23-472 • https://www.fortiguard.com/psirt/FG-IR-24-036

Affected Product	**Intel**
Severity	**Low**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2024-27457)
Description	Intel has released a security update addressing an Information Disclosure Vulnerability in Intel TDX Module firmware. An improper check for unusual or exceptional conditions in versions before Intel TDX Module firmware 1.5.06 may allow a privileged user to potentially enable information disclosure via local access. Intel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Intel TDX Module firmware before version 1.5.06.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01099.html

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.