Advisory Alert

Alert Number: AAA20241113 **Date:** November 13, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
Ivanti	**High**, **Medium**	Multiple Vulnerabilities
Citrix	**High**, **Medium**	Multiple Vulnerabilities
SAP	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Intel	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Dell	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Fortiguard	**High**, **Medium**, **Low**	Multiple Vulnerabilities
HPE	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**Medium**	Multiple Vulnerabilities
Zimbra	**Medium**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-50330 , CVE-2024-38655, CVE-2024-38656, CVE-2024-39710, CVE-2024-39711, CVE-2024-39712, CVE-2024-11007, CVE-2024-11006, CVE-2024-11005)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Remote Code Execution. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Ivanti Connect Secure before version 22.7R2.2 and 9.1R18.9 Ivanti Policy Secure before version 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-ICS-Ivanti-Policy-Secure-IPS-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs?language=en_US • https://forums.ivanti.com/s/article/Security-Advisory-EPM-November-2024-for-EPM-2024-and-EPM-2022?language=en_US

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-5535, CVE-2024-49056, CVE-2024-49051, CVE-2024-49050, CVE-2024-49049, CVE-2024-49048, CVE-2024-49046, CVE-2024-49044, CVE-2024-49043, CVE-2024-49042, CVE-2024-49040, CVE-2024-49039, CVE-2024-49033, CVE-2024-49032, CVE-2024-49031, CVE-2024-49030, CVE-2024-49029, CVE-2024-49028, CVE-2024-49027, CVE-2024-49026, CVE-2024-49021, CVE-2024-49019, CVE-2024-49018, CVE-2024-49017, CVE-2024-49016, CVE-2024-49015, CVE-2024-49014, CVE-2024-49013, CVE-2024-49012, CVE-2024-49011, CVE-2024-49010, CVE-2024-49009, CVE-2024-49008, CVE-2024-49007, CVE-2024-49006, CVE-2024-49005, CVE-2024-49004, CVE-2024-49003, CVE-2024-49002, CVE-2024-49001, CVE-2024-49000, CVE-2024-48999, CVE-2024-48998, CVE-2024-48997, CVE-2024-48996, CVE-2024-48995, CVE-2024-48994, CVE-2024-48993, CVE-2024-43646, CVE-2024-43645, CVE-2024-43644, CVE-2024-43643, CVE-2024-43642, CVE-2024-43641, CVE-2024-43640, CVE-2024-43639, CVE-2024-43638, CVE-2024-43637, CVE-2024-43636, CVE-2024-43635, CVE-2024-43634, CVE-2024-43633, CVE-2024-43631, CVE-2024-43630, CVE-2024-43629, CVE-2024-43628, CVE-2024-43627, CVE-2024-43626, CVE-2024-43625, CVE-2024-43624, CVE-2024-43623, CVE-2024-43622, CVE-2024-43621, CVE-2024-43620, CVE-2024-43613, CVE-2024-43602, CVE-2024-43598, CVE-2024-43530, CVE-2024-43499, CVE-2024-43498, CVE-2024-43462, CVE-2024-43459, CVE-2024-43452, CVE-2024-43451, CVE-2024-43450, CVE-2024-43449, CVE-2024-43447, CVE-2024-38264, CVE-2024-38255, CVE-2024-38203, CVE-2024-10827, CVE-2024-10826)
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, Privilege Escalation, Denial of Service Microsoft advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	.NET 9.0 Azure CycleCloud 8.0.0, 8.0.1, 8.0.2, 8.1.0, 8.1.1, 8.2.0, 8.2.1, 8.2.2, 8.3.0, 8.4.0, 8.4.1, 8.4.2, 8.5.0, 8.6.0, 8.6.1, 8.6.2, 8.6.3, 8.6.4 Azure Database for PostgreSQL Flexible Server 12, 13, 14, 15, 16 Azure Linux 3.0 ARM Azure Linux 3.0 x64 CBL Mariner 2.0 ARM CBL Mariner 2.0 x64 LightGBM Microsoft 365 Apps for Enterprise (32-bit / 64-bit) Microsoft Defender for Endpoint for Android Microsoft Defender for Endpoint for iOS Microsoft Edge (Chromium-based) Microsoft Excel 2016 (32-bit edition) Microsoft Excel 2016 (64-bit edition) Microsoft Excel 2016 Click-to-Run (C2R) for 32-bit editions Microsoft Excel 2016 Click-to-Run (C2R) for 64-bit editions Microsoft Exchange Server 2016 Cumulative Update 23 Microsoft Exchange Server 2019 Cumulative Update 13 Microsoft Exchange Server 2019 Cumulative Update 14 Microsoft Office 2016 (32-bit / 64-bit) Microsoft Office 2019 (32-bit / 64-bit) Microsoft Office LTSC 2021 (32-bit / 64-bit) Microsoft Office LTSC 2024 (32-bit / 64-bit) Microsoft Office LTSC for Mac (2021 / 2024) Microsoft Office Online Server Microsoft PC Manager Microsoft SharePoint Enterprise Server 2016 Microsoft SharePoint Server 2019 Microsoft SharePoint Server Subscription Edition Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR) Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 Azure Connect Feature Pack Microsoft SQL Server 2017 for x64-based Systems (CU 31) / (GDR) Microsoft SQL Server 2019 for x64-based Systems (CU 29) / (GDR) Microsoft SQL Server 2022 for x64-based Systems (CU 15) / (GDR) Microsoft TorchGeo	Microsoft Visual Studio 2022 version 17.10 Microsoft Visual Studio 2022 version 17.11 Microsoft Visual Studio 2022 version 17.6 Microsoft Visual Studio 2022 version 17.8 Microsoft Word 2016 (32-bit edition) Microsoft Word 2016 (64-bit edition) Python extension for Visual Studio Code Visual Studio Code Remote - SSH Extension 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 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 / Server Core Windows Server 2012 R2 / Server Core Windows Server 2016 / Server Core Windows Server 2019 / Server Core Windows Server 2022 / Server Core Windows Server 2022, 23H2 (Server Core) Windows Server 2025 / Server Core
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2024-Nov

Affected Product	**Ivanti**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-50317, CVE-2024-50318, CVE-2024-50319, CVE-2024-50320, CVE-2024-50321, CVE-2024-50331, CVE-2024-47905, CVE-2024-37400, CVE-2024-9420, CVE-2024-47906, CVE-2024-47907, CVE-2024-47909, CVE-2024-8495, CVE-2024-38649, CVE-2024-38655, CVE-2024-38656, CVE-2024-39709, CVE-2024-39710, CVE-2024-39711, CVE-2024-39712, CVE-2024-11007, CVE-2024-11006, CVE-2024-11005, CVE-2024-11004, CVE-2024-8539, CVE-2024-38654, CVE-2024-9842, CVE-2024-9843, CVE-2024-29211, CVE-2024-37398, CVE-2024-7571, CVE-2024-34787, CVE-2024-50322, CVE-2024-32839, CVE-2024-32841, CVE-2024-32844, CVE-2024-32847, CVE-2024-34780, CVE-2024-37376, CVE-2024-34781, CVE-2024-34782, CVE-2024-34784, CVE-2024-50323, CVE-2024-50324, CVE-2024-50326, CVE-2024-50327, CVE-2024-50328, CVE-2024-50329, CVE-2024-50330)
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, Remote Code Execution, Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Endpoint Manager (EPM) 2024 September security update and prior, Ivanti Endpoint Manager (EPM) 2022 SU6 September security update and prior Ivanti Connect Secure (ICS) 22.7R2.2 and prior Ivanti Policy Secure (IPS) 22.7R1.1 and prior Ivanti Secure Access Client (ISAC) 22.7R3 and prior Ivanti Avalanche 6.4.5 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-Multiple-CVEs-Q4-2024-Release?language=en_US • https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs?language=en_US • https://forums.ivanti.com/s/article/Security-Advisory-EPM-November-2024-for-EPM-2024-and-EPM-2022?language=en_US

Affected Product	**Citrix**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45818, CVE-2024-8534, CVE-2024-8535, CVE-2024-8068, CVE-2024-8069)
Description	Citrix has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to memory corruption, Denial of Service, Privilege escalation, Remote Code Execution Citrix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• XenServer 8 • Citrix Hypervisor 8.2 CU1 LTSR • NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-29.72 • NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-55.34 • NetScaler ADC 13.1-FIPS BEFORE 13.1-37.207 • NetScaler ADC 12.1-FIPS BEFORE 12.1-55.321 • NetScaler ADC 12.1-NDcPP BEFORE 12.1-55.321 • Citrix Session Recording Citrix Virtual Apps and Desktops before 2407 hotfix 24.5.200.8 Current Release (CR) • Long Term Service Release (LTSR) Citrix Virtual Apps and Desktops 1912 LTSR before CU9 hotfix 19.12.9100.6 Citrix Virtual Apps and Desktops 2203 LTSR before CU5 hotfix 22.03.5100.11 Citrix Virtual Apps and Desktops 2402 LTSR before CU1 hotfix 24.02.1200.16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.citrix.com/s/article/CTX692065-xenserver-and-citrix-hypervisor-security-update-for-cve202445818?language=en_US • https://support.citrix.com/s/article/CTX691608-netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20248534-and-cve20248535?language=en_US • https://support.citrix.com/s/article/CTX691941-citrix-session-recording-security-bulletin-for-cve20248068-and-cve20248069?language=en_US

Affected Product	**SAP**
Severity	**High**, **Medium** , **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-47590, CVE-2024-39592, CVE-2024-42372, CVE-2024-47595, CVE-2024-47592, CVE-2024-47586, CVE-2024-47588, CVE-2024-47593, CVE-2024-47587, CVE-2024-33000)
Description	SAP has released security updates addressing multiple vulnerabilities that exist in their products. Malicious users could exploit these vulnerabilities to cause Information Disclosure, Cross-Site Scripting, Local Privilege Escalation, NULL Pointer Dereference SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP Web Dispatcher – Versions: WEBDISP 7.77, 7.89, 7.93, KERNEL 7.77, 7.89, 7.93, 9.12, 9.13 • SAP PDCE – Versions: S4CORE 102, 103, S4COREOP 104, 105, 106, 107, 108 • SAP NetWeaver AS Java (System Landscape Directory) – Versions: LM-SLD 7.5 • SAP Host Agent – Version: SAPHOSTAGENT 7.22 • SAP NetWeaver Application Server Java (Logon Application) – Versions: SERVERCORE 7.5 • 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, 8.04, 9.12, 9.13 • SAP NetWeaver Java (Software Update Manager) – Version: SUM 1.1 • SAP NetWeaver Application Server ABAP – Versions: KRNL64UC 7.53, KERNEL 7.53, 7.54, 7.77, 7.89, 7.93, 9.12 • SAP Cash Management (Cash Operations) – Versions: S4CORE 103, 104, 105, 106, 107, 108 • SAP Bank Account Management – Versions: 100, 101, 102, 103, 104, 105, 106, 107, 108
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/november-2024.html

Affected Product	**Intel**
Severity	**High**, **Medium** , **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Intel has issued security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Improper Input Validation, Denial Of Service, Escalation Of Privilege, Information Disclosure. Intel 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.intel.com/content/www/us/en/security-center/default.html

Affected Product	**Dell**
Severity	**High**, **Medium**, **Low**
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 the affected system. Dell 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.dell.com/support/kbdoc/en-us/000226011/dsa-2024-272 • https://www.dell.com/support/kbdoc/en-us/000226605/dsa-2024-298 • https://www.dell.com/support/kbdoc/en-us/000227819/dsa-2024-361 • https://www.dell.com/support/kbdoc/en-us/000227992/dsa-2024-368 • https://www.dell.com/support/kbdoc/en-us/000227920/dsa-2024-364 • https://www.dell.com/support/kbdoc/en-us/000227762/dsa-2024-308-security-update-for-dell-poweredge-server-for-intel-august-2024-security-advisories-2024-3-ipu • https://www.dell.com/support/kbdoc/en-us/000247691/dsa-2024-385-dell-poweredge-server-security-update-for-intel-tdx-module-software-vulnerability • https://www.dell.com/support/kbdoc/en-us/000225473/dsa-2024-241-security-update-for-dell-client-platform-for-intel-ethernet-controller-and-adapter-software-advisories

Affected Product	**Fortiguard**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-36507, CVE-2024-32117, CVE-2024-36509, CVE-2024-40592, CVE-2024-26011, CVE-2023-50176, CVE-2024-33505, CVE-2023-47543, CVE-2023-44255, CVE-2024-47574, CVE-2024-32118, CVE-2024-32116, CVE-2024-35274, CVE-2024-36513, CVE-2024-3596, CVE-2024-23666, CVE-2024-33510, CVE-2024-31496, CVE-2024-40590)
Description	Fortiguard has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Information Disclosure, Improper access control , Arbitrary Code Execution 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?product=FortiSwitchManager,FortiExtender,FortiSandbox,FortiAP-S,FortiCache,FortiSDNConnector,FortiTokenIOS,FortiSOAR,FortiPresence,FortiADC,FortiCloud,FortiAnalyzer-BigData,FortiFone,FortiConverter,FortiTokenAndroid,FortiWAN-Manager,FortiOS-6K7K,FortiIsolator,FortiAP-W2,FortiRecorder,FortiGuard,FortiAP-U,FortiAnalyzer,FortiMail,FortiAuthenticator,FortiTester,FortiWAN,FortiClientiOS,FortiOS,Meru%20Controller,FortiSIEMWindowsAgent,FortiAP-C,FSSO%20Windows%20DC%20Agent,FortiVoiceEnterprise,FortiClientAndroid,FortiWLM,FortiSIEM,FortiProxy,FortiClientEMS,AscenLink,FortiPortal,FortiClientLinux,FortiDDoS-F,FortiNAC,FortiDDoS,FortiClientMac,FortiAP,FortiNDR,FortiDDoS-CM,FortiWebManager,FortiWLC,FortiClientWindows,Meru%20AP,FortiSwitch,FSSO%20Windows%20CA,FortiDeceptor,FortiADCManager,FortiWeb,FortiManager,FortiEDR,FortiTokenMobileWP

Affected Product	**HPE**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-22351, CVE-2023-25546, CVE-2023-26551, CVE-2023-26552, CVE-2023-26553, CVE-2023-26554, CVE-2023-26555, CVE-2023-41833, CVE-2023-42772, CVE-2023-43753, CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237, CVE-2024-21781, CVE-2024-21820, CVE-2024-21829, CVE-2024-21850, CVE-2024-21853, CVE-2024-21871, CVE-2024-23599, CVE-2024-23918, CVE-2024-23984, CVE-2024-24968, CVE-2024-25565, CVE-2024-25585)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Unauthorized Access, Denial of Service, Buffer Overflow, Privilege escalation HPE 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://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04741en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04738en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04730en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04735en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04701en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04702en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04704en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04742en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04750en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04739en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04736en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04699en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbux04729en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04706en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04705en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbcr04732en_us&docLocale=en_US

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45085, CVE-2024-45072, CVE-2024-45071, CVE-2024-45086, CVE-2024-45087)
Description	IBM 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. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WebSphere Service Registry and Repository 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7175749 • https://www.ibm.com/support/pages/node/7175750 • https://www.ibm.com/support/pages/node/7175751 • https://www.ibm.com/support/pages/node/7175752 • https://www.ibm.com/support/pages/node/7175765

Affected Product	**Zimbra**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-22067, CVE-2023-38709, CVE-2024-20328)
Description	Zimbra has issued security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause sensitive Information Disclosure, arbitrary commands execution. Zimbra advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Zimbra Daffodil versions before (v10.1.3) Zimbra Collaboration Daffodil versions before 10.0.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.3#Security_Fixes • https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.11#Security_Fixes

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-48695, CVE-2023-52522, CVE-2024-26640, CVE-2024-26656, CVE-2024-26772, CVE-2024-26870, CVE-2024-26906, CVE-2024-31076, CVE-2024-40931, CVE-2024-41039, CVE-2024-42271, CVE-2024-46858)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Denial Of Service, Use After Free Condition, Improper Input Validation, Buffer Overflow Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:9497 • https://access.redhat.com/errata/RHSA-2024:9498 • https://access.redhat.com/errata/RHSA-2024:9500

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.