Advisory Alert

Alert Number: **AAA20240710** **Date:** **July 10, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Citrix	**Critical**	Multiple Vulnerabilities
HPE	**Critical**	Authentication Bypass vulnerability
IBM	**Critical**	SQL Injection Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
Juniper	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Dell	**High**	Security Update
Lenovo	**High**, **Low**	Multiple Vulnerabilities
Red Hat	**High**, **Low**	Multiple Vulnerabilities
SAP	**High**, **Medium**, **Low**	Multiple Vulnerabilities
FortiGuard	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Citrix	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Joomla	**Medium**, **Low**	Multiple Cross-Site Scripting Vulnerabilities

Description

Affected Product	**Citrix**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-6235, CVE-2024-6236)
Description	Citrix has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Sensitive information disclosure and Denial of Service. Citrix strongly advises to apply security fixes at earliest to avoid problems.
Affected Products	NetScaler Console 14.1 before 14.1-25.53 NetScaler Console 13.1 before 13.1-53.22 NetScaler Console 13.0 before 13.0-92.31 NetScaler SVM 14.1 before 14.1-25.53 NetScaler SVM 13.1 before 13.1-53.17 NetScaler SVM 13.0 before 13.0-92.31 NetScaler Agent 14.1 before 14.1-25.53 NetScaler Agent 13.1 before 13.1-53.22 NetScaler Agent 13.0 before 13.0-92.31
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX677998/netscaler-console-agent-and-svm-security-bulletin-for-cve20246235-and-cve20246236

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass vulnerability (CVE-2024-3596)
Description	HPE has released security updates addressing an Authentication Bypass vulnerability that exist in their products caused due to RADIUS Protocol being Susceptible to Forgery Attacks. Exploitation of this vulnerability may allow attackers to access sensitive network resources without authentication. HPE strongly advises to apply security fixes at earliest to avoid problems.
Affected Products	Switches running AOS-CX 10.13.1030 and below WLAN Gateways and SD-WAN Gateways running ArubaOS 10 • 10.6.0.2 and below • 10.4.1.3 and below Mobility Controllers running ArubaOS 8 • 8.12.0.1 and below • 8.10.0.13 and below Airwave Management Platform 8.3.0.2 and below ClearPass Policy Manager • 6.12.1 and below • 6.11.8 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04662en_us&docLocale=en_US

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	SQL Injection Vulnerability (CVE-2024-1597)
Description	IBM has released security updates addressing an SQL Injection Vulnerability that exists in PostgreSQL JDBC Driver that in turn affect IBM products. A remote attacker could send specially crafted SQL statements when using the non-default connection property preferQueryMode=simple in combination with application code that has a vulnerable SQL that negates a parameter value, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM strongly advises to apply security fixes at earliest to avoid problems.
Affected Products	IBM Storage Scale 5.1.0.0 - 5.1.9.2 IBM Security QRadar EDR 3.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7150357 https://www.ibm.com/support/pages/node/7159867

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Microsoft has issued the security update for the month of July 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 strongly advises to apply security fixes at earliest to avoid problems.
Affected Products	Windows 11 version 21H2 for x64-based / ARM64-based Systems Windows 11 Version 22H2 for x64-based / ARM64-based Systems Windows 11 Version 23H2 for x64-based / ARM64-based Systems Windows 10 Version 22H2 for 32-bit Systems / ARM64-based / x64-based Systems Windows 10 Version 21H2 for 32-bit / x64-based / ARM64-based Systems Windows 10 Version 1607 for 32-bit / x64-based Systems Windows 10 Version 1809 for 32-bit / x64-based / ARM64-based Systems Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2016 Windows Server 2019 Windows Server 2022, 23H2 Edition (Server Core installation) Microsoft Visual Studio 2022 version 17.4 17.6 /17.8 / 17.10 Azure CycleCloud 7.9.2 / 7.9.4 /7.9.6 / 7.9.5 / 7.9.10 / 7.9.11 / 8.0.1 Microsoft Defender for IoT . Microsoft NET 8.0 Microsoft .NET Framework 3.5 / 3.5.1 / 4.7.2 / 4.8 / 4.6 / 4.6.2/4.7/4.7.1/4.7.2 Microsoft .NET Framework 2.0 AND 3.0 Service Pack 2 Microsoft .NET Framework 3.5 AND 4.8.1 Microsoft 365 Apps for Enterprise for 32-bit AND 64-bit Systems Microsoft Office 2019 for 32-bit AND 64-bit editions Microsoft SharePoint Server Subscription Edition Microsoft SharePoint Server 2019 Microsoft SharePoint Enterprise Server 2016 Azure CycleCloud 7.9.0 -7.9.9 AND 8.1.0 - 8.5.0 Microsoft Office 2016 32-bit / 64-bit editions Microsoft Office LTSC 2021 for 32-bit / 64-bit editions Microsoft Outlook 2016 32-bit / 64-bit Editions Systems Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR) Microsoft SQL Server 2017 / 2019 / 2022 for x64-based Systems (CU 13/27/31) (GDR) Service Pack 3 Azure Connect Feature Pack Microsoft SQL Server 2017 / 2019 for x64-based Systems (GDR) Microsoft OLE DB Driver 18 / 19 for SQL Server Azure DevOps Server 2022.1 Azure Network Watcher VM Extension for Windows Azure Kinect SDK Microsoft Dynamics 365 (on-premises) version 9.1 Microsoft Edge (Chromium-based) / Android / iOS Microsoft Power Platform Microsoft Dynamics 365 Business Central 2023 Release Wave 1 Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10) Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8) Azure Data Science Virtual Machines for Linux Azure Monitor Agent Azure File Sync v16.0 / v17.0 / v18.0 Azure Storage Movement Client Library for .NET Microsoft Dynamics 365 Business Central 2023 Release Wave 2 Microsoft Dynamics 365 Business Central 2024 Release Wave 1 Azure Identity Library for Python Azure Identity Library for C++ Azure Identity Library for JavaScript Microsoft Authentication Library (MSAL) for Node.js Microsoft Authentication Library (MSAL) for .NET Azure Identity Library for Go Microsoft Authentication Library (MSAL) for Java Azure Identity Library for .NET
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2024-Jul

Affected Product	**Juniper**
Severity	**Critical -** Initial release date **8th February 2024 (AAA20240208)**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2023-35116, CVE-2023-34453, CVE-2023-34455, CVE-2023-34454, CVE-2023-43642, CVE-2023-2976, CVE-2023-33201, CVE-2023-46136, CVE-2023-43804, CVE-2023-37920, CVE-2022-25883, CVE-2023-45133, CVE-2023-31484, CVE-2023-1370, CVE-2021-4048, CVE-2021-23445, CVE-2021-31684, CVE-2023-38019, CVE-2023-38020, CVE-2023-38263, CVE-2023-46308, CVE-2023-32006, CVE-2023-32002, CVE-2023-32559, CVE-2022-38900, CVE-2023-45857, CVE-2022-25927, CVE-2023-44270, CVE-2023-26159, CVE-2020-19909, CVE-2023-38546, CVE-2023-38545, CVE-2023-5678, CVE-2023-46218, CVE-2023-46219, CVE-2023-4807, CVE-2023-0727, CVE-2023-6129, CVE-2023-5363, CVE-2022-21216, CVE-2023-46234, CVE-2024-28849, CVE-2024-29041, CVE-2024-29180, CVE-2024-4067, CVE-2024-4068)
Description	Juniper has released a security update addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to denial of service, integer overflow, LDAP injection, Improper Input Validation. Juniper strongly advises to apply security fixes at earliest to avoid problems.
Affected Products	Log Collector Application prior to version v1.8.4 SOAR Plugin Application prior to version 5.3.1 Deployment Intelligence Application prior to 3.0.13 User Behavior Analytics Application add-on prior to 4.1.14 Pulse Application add-on prior to 2.2.12 Assistant Application add-on prior to 3.6.0 Use Case Manager Application add-on prior to 3.9.0 WinCollect Standalone Agent prior to 10.1.8 M7 Appliances prior to 4.0.0 Log Source Management App prior to 7.0.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-JSA-Series-Multiple-vulnerabilities-resolved-in-JSA-Applications?language=en_US

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Out of bound access, Denial of Service, Privilege escalation, Use-after-free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3, 15.5 Public Cloud Module 15-SP5 SUSE Linux Enterprise High Performance Computing 15 SP2, 15 SP3, 15 SP5 SUSE Linux Enterprise Live Patching 15-SP2, 15-SP3 SUSE Linux Enterprise Micro 5.1, 5.2, 5.5 SUSE Linux Enterprise Server 15 SP2, 15 SP3, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP2, 15 SP3, 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20242369-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242368-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242372-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242373-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242376-1/

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2024-5460)
Description	Dell has released a security update addressing a vulnerability that exists in Brocade Fabric OS third-party product that in turn affect Dell products. The vulnerability exists in the default configuration of the Simple Network Management Protocol (SNMP) feature of Brocade Fabric OS versions before v9.0.0, this could allow an authenticated, remote attacker to read data from an affected device via SNMP. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FOS Versions 7.x, 8.x that exists in • Connectrix ED-DCX8510-4B • Connectrix ED-DCX8510-8B • Connectrix DS-6520B • Connectrix DS-6510B • Connectrix DS-6505B • Connectrix MP-7840B
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000226787/dsa-2024-234-security-update-for-dell-connectrix-brocade-for-snmpv1-vulnerability

Affected Product	**Lenovo**
Severity	**High**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38508, CVE-2024-38509, CVE-2024-38510, CVE-2024-38511, CVE-2024-38512, CVE-2018-25103)
Description	Lenovo has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Privilege escalation and Use after free conditions. Lenovo 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.lenovo.com/us/en/product_security/LEN-156781 • https://support.lenovo.com/us/en/product_security/LEN-158417

Affected Product	**Red Hat**
Severity	**High**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Remote Code Execution, Memory Leak, Data Injection, Use-after-free conditions. 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 8 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 8 s390x Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for Real Time 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.0 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.0 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 9.0 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.0 s390x 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 9.0 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:4352 • https://access.redhat.com/errata/RHSA-2024:4412 • https://access.redhat.com/errata/RHSA-2024:4415 • https://access.redhat.com/errata/RHSA-2024:4447 • https://access.redhat.com/errata/RHSA-2024:4351

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-34683, CVE-2024-34685, CVE-2024-34689, CVE-2024-34692, CVE-2024-37171, CVE-2024-37172, CVE-2024-37173, CVE-2024-37174, CVE-2024-37175, CVE-2024-37180, CVE-2024-39592, CVE-2024-39593, CVE-2024-39594, CVE-2024-39596, CVE-2024-39597, CVE-2024-39598, CVE-2024-39600)
Description	SAP has issued monthly security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Information Disclosure, Cross-Site Scripting, Server-Side Request Forgery (SSRF). SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SAP PDCE, Version – S4CORE 102, 103, S4COREOP 104, 105, 106, 107, 108 SAP Commerce, Version – HY_COM 2205, COM_CLOUD 2211 SAP Landscape Management, Version - VCM 3.00 SAP Document Builder, Versions – • S4CORE 100, 101, S4FND 102, 103, 104, 105, 106, 107, 108, SAP_BS_FND 702, 731, 746, 747, 748 SAP NetWeaver Knowledge Management XMLEditor, Version – KMC-WPC 7.50 SAP CRM WebClient UI, Versions – • S4FND 102, 103, 104, 105, 106, 107, 108, WEBCUIF 701, 731, 746, 747, 748, 800, 801 SAP Business Warehouse - Business Planning and Simulation Versions – • SAP_BW 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 758, SAP_BW_VIRTUAL_COMP 701 SAP S/4HANA Finance (Advanced Payment Management), Versions – S4CORE 107, 108 SAP Business Workflow (WebFlow Services), 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 Business Workflow (WebFlow Services), 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 Business Workflow (WebFlow Services), 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 GUI for Windows, Version – BC-FES-GUI 8 SAP Transportation Management (Collaboration Portal), Versions – SAPTMUI 140, 150, 160, 170 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_BASIS 758, SAP_BASIS 795, SAP_BASIS 796 SAP Enable Now, Versions – • WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704 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 SAP CRM WebClient UI, Versions – S4FND 104 SAP Enable Now, Versions – • WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/content/dam/support/en_us/library/ssp/my-support/knowledge-base/security-notes-news/2024%2007%20Patch%20Day%20Blog%20V1.pdf

Affected Product	**FortiGuard**	
Severity	**High**, **Medium**, **Low**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-33509, CVE-2023-50179, CVE-2024-23663, CVE-2023-50178, CVE-2024-21759, CVE-2023-50181, CVE-2024-26015, CVE-2024-26006)	
Description	FortiGuard has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Cross-Site Scripting, Information disclosure, Improper access control and Unauthorized command and code execution. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.	
Affected Products	FortiADC 6.0 all versions FortiADC 6.1 all versions FortiADC 6.2 all versions FortiADC 7.0 all versions FortiADC 7.1 all versions FortiADC 7.2 all versions FortiADC 7.4.0 through 7.4.1 FortiExtender 7.0.0 through 7.0.4 FortiExtender 7.2.0 through 7.2.4 FortiExtender 7.4.0 through 7.4.2 FortiOS 7.0 all versions FortiOS 7.2 all versions	FortiOS 7.4.0 through 7.4.3 FortiPortal 7.0.0 through 7.0.6 FortiPortal 7.2.0 FortiProxy 7.0 all versions FortiProxy 7.0.0 through 7.0.16 FortiProxy 7.2 all versions FortiProxy 7.4.0 through 7.4.3 FortiWeb 6.3 all versions FortiWeb 6.4 all versions FortiWeb 7.0 all versions FortiWeb 7.2.0 through 7.2.1
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	• https://www.fortiguard.com/psirt/FG-IR-22-326 • https://www.fortiguard.com/psirt/FG-IR-23-480 • https://www.fortiguard.com/psirt/FG-IR-23-459 • https://www.fortiguard.com/psirt/FG-IR-22-298 • https://www.fortiguard.com/psirt/FG-IR-24-011 • https://www.fortiguard.com/psirt/FG-IR-23-469 • https://www.fortiguard.com/psirt/FG-IR-23-446 • https://www.fortiguard.com/psirt/FG-IR-23-485	

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45803, CVE-2023-5752, CVE-2024-28102, CVE-2024-28849, CVE-2024-28863, CVE-2024-28176, CVE-2024-27088, CVE-2024-4067, CVE-2024-4603, CVE-2024-2466, CVE-2024-4068, CVE-2024-4741, CVE-2024-2379, CVE-2024-2004, CVE-2024-2511, CVE-2024-2398)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Execute Arbitrary Code Execution, Sensitive Information disclosure, Bypass of TLS Certificate Checks. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security QRadar EDR Version - 3.12 QRadar WinCollect Agent Version - 10.0-10.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7159867 • https://www.ibm.com/support/pages/node/7159865

Affected Product	**Citrix**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-6286, CVE-2024-6151, CVE-2024-6150, CVE-2024-6149, CVE-2024-6148, CVE-2024-5492, CVE-2024-5491)
Description	Citrix has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Local Privilege Escalation, System Disruption, Policy Bypass, Denial of Service conditions. Citrix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Citrix Workspace app for Windows versions before 2403.1 (Current Release) Citrix Workspace app for Windows versions before 2402 LTSR (Long Term Service Release) Citrix Workspace app for HTML5 before 2404.1 Citrix Virtual Apps and Desktops versions before 2402 (Current Release) Citrix Virtual Apps and Desktops 1912 LTSR before CU9 (Long Term Service Release) Citrix Virtual Apps and Desktops 2203 LTSR before CU5 (Long Term Service Release) Citrix Provisioning versions before 2402 (Current Release) Citrix Provisioning versions before 2203 LTSR CU5 (Long Term Service Release) Citrix Provisioning versions before 1912 LTSR CU9 (Long Term Service Release) NetScaler ADC and NetScaler Gateway 14.1 before 14.1-25.53 NetScaler ADC and NetScaler Gateway 13.1 before 13.1-53.17 NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.31 NetScaler ADC 13.1-FIPS before 13.1-37.183 NetScaler ADC 12.1-FIPS before 12.1-55.304 NetScaler ADC 12.1-NDcPP before 12.1-55.304
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.citrix.com/article/CTX678036/citrix-workspace-app-for-windows-security-bulletin-cve20246286 • https://support.citrix.com/article/CTX678035/windows-virtual-delivery-agent-for-cvad-and-citrix-daas-security-bulletin-cve20246151 • https://support.citrix.com/article/CTX678025/citrix-provisioning-security-bulletin-cve20246150 • https://support.citrix.com/article/CTX678037/citrix-workspace-app-for-html5-security-bulletin-cve20246148-and-cve20246149 • https://support.citrix.com/article/CTX677944/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20245491-and-cve20245492

Affected Product	**Joomla**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Cross-Site Scripting Vulnerabilities (CVE-2024-26279, CVE-2024-26278, CVE-2024-21731, CVE-2024-21730, CVE-2024-21729)
Description	Joomla has released security updates addressing multiple Cross-Site Scripting Vulnerabilities that exist in their products. Exploitation of these vulnerabilities may allow a malicious user to compromise the affected systems. Joomla advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Joomla! CMS versions 3.0.0-3.10.15-elts, 4.0.0-4.4.5, 5.0.0-5.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://developer.joomla.org/security-centre/939-20240705-core-xss-in-com-fields-default-field-value.html • https://developer.joomla.org/security-centre/938-20240704-core-xss-in-wrapper-extensions.html • https://developer.joomla.org/security-centre/937-20240703-core-xss-in-stringhelper-truncate-method.html • https://developer.joomla.org/security-centre/936-20240702-core-self-xss-in-fancyselect-list-field-layout.html • https://developer.joomla.org/security-centre/935-20240701-core-xss-in-accessible-media-selection-field.html

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.