Advisory Alert

Alert Number: AAA20231213 **Date:** December 13, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Path traversal Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
Fortiguard	**Critical**	Improper Access Control Vulnerability
Fortiguard	**High** , **Medium** , **Low**	Multiple Vulnerabilities
IBM	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Path traversal Vulnerability (CVE-2023-50164)
Description	Cisco has released security updates addressing Apache Struts disclosed directory traversal vulnerability in their products. An attacker can manipulate file upload params to enable paths traversal and under some circumstances this can lead to uploading a malicious file which can be used to perform Remote Code Execution. Cisco highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Customer Collaboration Platform, formerly SocialMiner Identity Services Engine (ISE) Security Manager Nexus Dashboard Fabric Controller (NDFC), formerly Data Center Network Manager (DCNM) Prime Access Registrar Prime Collaboration Assurance Prime Collaboration Provisioning Prime Infrastructure Prime License Manager Prime Service Catalog Computer Telephony Integration Object Server (CTIOS) Emergency Responder Enterprise Chat and Email Finesse Hosted Collaboration Mediation Fulfillment Unified Communications Manager (Unified CM) / Unified Communications Manager Session Management Edition (Unified CM SME) Unified Communications Manager IM & Presence Service (Unified CM IM&P) Unified Contact Center Enterprise (Unified CCE) Unified Contact Center Enterprise - Live Data server (Unified CCE - Live Data Server) Unified Contact Center Express (Unified CCX) Unified Customer Voice Portal (Unified CVP) Unified Intelligence Center Unified Intelligent Contact Management Enterprise Unified SIP Proxy Software Unity Connection Unity Express Virtualized Voice Browser
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-struts-C2kCMkmT https://cwiki.apache.org/confluence/display/WW/S2-066

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-35621, CVE-2023-35622, CVE-2023-35619, CVE-2023-20588, CVE-2023-36696, CVE-2023-35635, CVE-2023-35633, CVE-2023-35632, CVE-2023-35631, CVE-2023-35630, CVE-2023-35629, CVE-2023-35628, CVE-2023-35643, CVE-2023-35642, CVE-2023-35641, CVE-2023-35639, CVE-2023-35638, CVE-2023-36006, CVE-2023-36005, CVE-2023-36004, CVE-2023-36003, CVE-2023-36011, CVE-2023-36009, CVE-2023-21740, CVE-2023-35644, CVE-2023-36012, CVE-2023-35634, CVE-2023-35621, CVE-2023-35628, CVE-2023-35636, CVE-2023-35610, CVE-2023-36391, CVE-2023-36696.)
Description	Microsoft has issued the security update for the month of December addressing critical multiple vulnerabilities that exists in variety of Microsoft products. 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 earliest to avoid problems.
Affected Products	Azure Connected Machine Agent Azure Machine Learning Microsoft Bluetooth Driver Microsoft Dynamics Microsoft Edge (Chromium-based) Microsoft Office Outlook Microsoft Office Word Microsoft Power Platform Connector Microsoft WDAC OLE DB provider for SQL Microsoft Windows DNS Windows Cloud Files Mini Filter Driver Windows Defender Windows DHCP Server Windows DPAPI (Data Protection Application Programming Interface) Windows Internet Connection Sharing (ICS) Windows Kernel Windows Kernel-Mode Drivers Windows Local Security Authority Subsystem Service (LSASS) Windows Media Windows MSHTML Platform Windows ODBC Driver Windows Telephony Server Windows USB Mass Storage Class Driver Windows Win32K XAML Diagnostics
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2023-Dec

Affected Product	**Fortiguard**
Severity	**Critical**
Affected Vulnerability	Improper Access Control Vulnerability (CVE-2023-47539)
Description	Fortiguard has issued the security update for Improper Access Control Vulnerability that exists in the FortiMail. An improper access control vulnerability in FortiMail configured with RADIUS authentication and remote_wildcard enabled may allow a remote unauthenticated attacker to bypass admin login via a crafted HTTP request. Fortiguard advises to apply security fixes at earliest to avoid problems.
Affected Products	FortiMail 7.4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-439

Affected Product	**Fortiguard**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-41678, CVE-2023-41673, CVE-2022-27488, CVE-2023-47536, CVE-2023-36639, CVE-2023-48791, CVE-2023-41844, CVE-2023-45587, CVE-2023-40716, CVE-2023-48782, CVE-2023-46713)
Description	Fortiguard has released security updates addressing multiple vulnerabilities that exists in their products including an improper privilege management, command injection, cross-site scripting, information leakage, improper verification, path traversal, privilege escalation, arbitrary code execute and Inject script. It is recommended by Fortiguard to apply necessary security fixes at earliest to avoid issues
Affected Products	FortiADC 6.0 6.0 all versions FortiADC 6.1 6.1 all versions FortiADC 6.2 6.2 all versions FortiADC 7.0 7.0 all versions FortiADC 7.1 7.1 all versions FortiADC 7.2 7.2.0 through 7.2.2 FortiADC 7.4 7.4.0 FortiMail 6.0 6.0 all versions FortiMail 6.2 6.2 all versions FortiMail 6.4 6.4.0 through 6.4.6 FortiMail 7.0 7.0.0 through 7.0.3 FortiNDR 1.1 1.1 all versions FortiNDR 1.2 1.2 all versions FortiNDR 1.3 1.3 all versions FortiNDR 1.4 1.4 all versions FortiNDR 1.5 1.5 all versions FortiNDR 7.0 7.0.0 through 7.0.4 FortiNDR 7.1 7.1.0 FortiOS 6.0 6.0 all versions FortiOS 6.2 6.2.0 through 6.2.15 FortiOS 6.4 6.4 all versions FortiOS 7.0 7.0 all versions FortiOS 7.2 7.2.0 FortiOS 7.2 7.2.0 through 7.2.4 FortiOS 7.4 7.4.0 FortiPAM 1.0 1.0 all versions FortiPAM 1.1 1.1.0 through 1.1.1 FortiPortal 7.0 7.0.0 through 7.0.6 FortiPortal 7.2 7.2.0 FortiProxy 2.0 2.0.0 through 2.0.12 FortiProxy 7.0 7.0.0 through 7.0.10 FortiProxy 7.2 7.2.0 through 7.2.4 FortiRecorder 2.6 2.6 all versions FortiRecorder 2.7 2.7 all versions FortiRecorder 6.0 6.0.0 through 6.0.11 FortiRecorder 6.4 6.4.0 through 6.4.2 FortiSandbox 3.0 3.0.4 and above FortiSandbox 3.1 3.1 all versions	FortiSandbox 4.4 4.4.0 through 4.4.2 FortiSandbox 3.2 3.2 all versions FortiSandbox 4.0 4.0 all versions FortiSandbox 4.2 4.2 all versions FortiSwitch 6.0 6.0 all versions FortiSwitch 6.2 6.2 all versions FortiSwitch 6.4 6.4.0 through 6.4.10 FortiSwitch 7.0 7.0.0 through 7.0.4 FortiTester 2.3 2.3 all versions FortiTester 2.4 2.4 all versions FortiTester 2.5 2.5 all versions FortiTester 2.6 2.6 all versions FortiTester 2.7 2.7 all versions FortiTester 2.8 2.8 all versions FortiTester 2.9 2.9 all versions FortiTester 3.0 3.0 all versions FortiTester 3.1 3.1 all versions FortiTester 3.2 3.2 all versions FortiTester 3.3 3.3 all versions FortiTester 3.4 3.4 all versions FortiTester 3.5 3.5 all versions FortiTester 3.6 3.6 all versions FortiTester 3.7 3.7 all versions FortiTester 3.8 3.8 all versions FortiTester 3.9 3.9 all versions FortiTester 4.0 4.0 all versions FortiTester 4.1 4.1 all versions FortiTester 4.2 4.2 all versions FortiTester 7.0 7.0 all versions FortiTester 7.1 7.1 all versions FortiTester 7.2 7.2 all versions FortiVoice 6.0 6.0.0 through 6.0.11 FortiVoice 6.4 6.4.0 through 6.4.7 FortiWeb 6.2 6.2 all versions FortiWeb 6.3 6.3 all versions FortiWeb 7.0 7.0 all versions FortiWeb 7.2 7.2.0 through 7.2.5 FortiWeb 7.4 7.4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt

Affected Product	**IBM**
Severity	**Medium** , **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1370, CVE-2022-3171, CVE-2022-3509, CVE-2023-43642, CVE-2023-34462, CVE-2023-32731, CVE-2022-3510, CVE-2022-1471, CVE-2022-25857, CVE-2022-41854 CVE-2022-38752, CVE-2022-38750, CVE-2022-38749, CVE-2022-38751)
Description	IBM has released security updates addressing Multiple Vulnerabilities in DB2 product. IBM Db2 Federated is affected by vulnerabilities in open source libraries. Attackers could exploit these flaws for denial of service, arbitrary code execution, and sensitive information disclosure. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM Db2 11.1.4.x IBM Db2 11.5.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7087234 https://www.ibm.com/support/pages/node/7095807

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.