Advisory Alert

Alert Number: AAA20230412 **Date:** April 12, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
Fortinet	**Critical**	Missing Authentication vulnerability
SAP	**Critical**	Multiple Vulnerabilities
Ivanti	**High**	Denial of Service Vulnerabilities
Lenovo	**High**	Multiple Vulnerabilities
Fortinet	**High**, **Medium**, **Low**	Multiple Vulnerabilities
SAP	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**Medium**	Privilege Escalation Vulnerability

Description

Affected Product	**Microsoft**	
Severity	**Critical**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-21554, CVE-2023-21727, CVE-2023-21729, CVE-2023-23375, CVE-2023-23384, CVE-2023-24860, CVE-2023-24883, CVE-2023-24884, CVE-2023-24885, CVE-2023-24886, CVE-2023-24887, CVE-2023-24893, CVE-2023-24912, CVE-2023-24914, CVE-2023-24924, CVE-2023-24925, CVE-2023-24926, CVE-2023-24927, CVE-2023-24928, CVE-2023-24929, CVE-2023-24935, CVE-2023-28216, CVE-2023-28218, CVE-2023-28219, CVE-2023-28220, CVE-2023-28221, CVE-2023-28222, CVE-2023-28223, CVE-2023-28224, CVE-2023-28225, CVE-2023-28226, CVE-2023-28227, CVE-2023-28228, CVE-2023-28229, CVE-2023-28231, CVE-2023-28232, CVE-2023-28233, CVE-2023-28234, CVE-2023-28235, CVE-2023-28236, CVE-2023-28237, CVE-2023-28238, CVE-2023-28240, CVE-2023-28243, CVE-2023-28244, CVE-2023-28246, CVE-2023-28247, CVE-2023-28248, CVE-2023-28249, CVE-2023-28250, CVE-2023-28251, CVE-2023-28252, CVE-2023-28253, CVE-2023-28254, CVE-2023-28255, CVE-2023-28256, CVE-2023-28260, CVE-2023-28262, CVE-2023-28263, CVE-2023-28266, CVE-2023-28267, CVE-2023-28268, CVE-2023-28269, CVE-2023-28270, CVE-2023-28271, CVE-2023-28272, CVE-2023-28273, CVE-2023-28274, CVE-2023-28275, CVE-2023-28276, CVE-2023-28277, CVE-2023-28278, CVE-2023-28284, CVE-2023-28285, CVE-2023-28287, CVE-2023-28288, CVE-2023-28291, CVE-2023-28292, CVE-2023-28295, CVE-2023-28296, CVE-2023-28297, CVE-2023-28300, CVE-2023-28301, CVE-2023-28304, CVE-2023-28305, CVE-2023-28306, CVE-2023-28307, CVE-2023-28308, CVE-2023-28309, CVE-2023-28311, CVE-2023-28312, CVE-2023-28313, CVE-2023-28314)	
Description	Microsoft has issued the security update for the month of April 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	.NET Core Azure Machine Learning Azure Service Connector Microsoft Bluetooth Driver Microsoft Defender for Endpoint Microsoft Dynamics Microsoft Dynamics 365 Customer Voice Microsoft Edge (Chromium-based) Microsoft Graphics Component Microsoft Message Queuing Microsoft Office Microsoft Office Publisher Microsoft Office SharePoint Microsoft Office Word Microsoft PostScript Printer Driver Microsoft Printer Drivers Microsoft WDAC OLE DB provider for SQL Microsoft Windows DNS Visual Studio Visual Studio Code Windows Active Directory Windows ALPC Windows Ancillary Function Driver for WinSock Windows Boot Manager Windows Clip Service Windows CNG Key Isolation Service Windows Common Log File System Driver	Windows DHCP Server Windows Enroll Engine Windows Error Reporting Windows Group Policy Windows Internet Key Exchange (IKE) Protocol Windows Kerberos Windows Kernel Windows Layer 2 Tunneling Protocol Windows Lock Screen Windows Netlogon Windows Network Address Translation (NAT) Windows Network File System Windows Network Load Balancing Windows NTLM Windows PGM Windows Point-to-Point Protocol over Ethernet (PPPoE) Windows Point-to-Point Tunneling Protocol Windows Raw Image Extension Windows RDP Client Windows Registry Windows RPC API Windows Secure Boot Windows Secure Channel Windows Secure Socket Tunneling Protocol (SSTP) Windows Transport Security Layer (TLS) Windows Win32K
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2023-Apr	

Affected Product	**Fortinet**
Severity	**Critical**
Affected Vulnerability	Missing Authentication vulnerability (CVE-2022-41331)
Description	Fortinet has released a security update addressing a Missing authentication vulnerability in FortiPresence infrastructure server. Exploitation of the vulnerability may allow a remote, unauthenticated attacker to access the Redis and MongoDB instances via crafted authentication requests. Fortinet highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	FortiPresence 1.2 all versions FortiPresence 1.1 all versions FortiPresence 1.0 all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-22-355

Affected Product	**Sap**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-27497, CVE-2023-27267, CVE-2022-41272, CVE-2023-28765, CVE-2023-27269)
Description	SAP has released a security update addressing multiple vulnerabilities in their products. If exploited these vulnerabilities could lead to Information disclosure, Directory traversal, Script execution, full read access to user data SAP highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	SAP Diagnostics Agent (OSCommand Bridge and EventLogServiceCollector),Version –720 SAP Business Client, Versions -6.5, 7.0, 7.70 SAP NetWeaver Process Integration, Version –7.50 SAP BusinessObjects Business Intelligence Platform (Promotion Management,Versions–420, 430 SAP NetWeaver Application Server for ABAP and ABAP Platform, Versions -700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=100

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerabilities (CVE-2022-35254, CVE-2022-35258)
Description	Ivanti has released security updates addressing Denial of Service vulnerabilities affecting their products. An unauthenticated attacker can cause denial-of-service in Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS), Ivanti Neurons for Zero-Trust Gateway Ivanti recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Ivanti Connect Secure (ICS) prior to 9.1R14.3, 9.1R15.2, 9.1R16.2, and 22.2R3 Ivanti Policy Secure (IPS) prior to 9.1R17 and 22.2R3 Ivanti Neurons for Zero-Trust Gateway prior to 22.3R1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/SA45520?language=en_US

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0896, CVE-2023-29056, CVE-2023-29057, CVE-2023-29058)
Description	Lenovo has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-0896** - A default password was reported in Lenovo Smart Clock Essential with Alexa Built In (Lenovo CD-4N342Y) that could allow unauthorized device access to an attacker with local network access. **CVE-2023-29056** - A valid LDAP user, under specific conditions, will default to read-only permissions when authenticating into XCC. To be vulnerable, XCC must be configured to use an LDAP server for Authentication/Authorization and have the login permission attribute not defined. **CVE-2023-29057** - A valid XCC user's local account permissions overrides their active directory permissions under specific configurations. This could lead to a privilege escalation. To be vulnerable, LDAP must be configured for authentication/authorization and logins configured as “Local First, then LDAP”. **CVE-2023-29058** - A valid, authenticated XCC user with read-only permissions can modify custom user roles on other user accounts and the user trespass message through the XCC CLI. There is no exposure if SSH is disabled or if there are no users assigned optional read-only permissions. Lenovo recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/us/en/product_security/LEN-118321 https://support.lenovo.com/us/en/product_security/LEN-113714

Affected Product	**Fortinet**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-0847, CVE-2022-40679, CVE-2022-40682, CVE-2022-43946, CVE-2022-42470, CVE-2022-41330, CVE-2023-27995, CVE-2022-27487, CVE-2022-43955, CVE-2023-22642, CVE-2022-42477, CVE-2022-35850, CVE-2023-22635, CVE-2022-42469, CVE-2022-43951, CVE-2022-43947, CVE-2023-22641, CVE-2022-27485, CVE-2022-43948, CVE-2022-43952)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of these vulnerabilities could lead to Cross-site scripting, Command injection, Arbitrary file creation, Server-side Template injection. Fortinet recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	FortiADC 5.1, 5.2, 5.3, 5.4, 6.0, 6.1, 6.2, all versions FortiADC version 5.x, 6.0, 6.1 all versions FortiADC version 6.2.0 through 6.2.4, 6.2.0 through 6.2.5, 7.0.0 through 7.0.3 FortiADC version 7.1.0 FortiADC version 7.1.0 through 7.1.1 FortiAnalyzer 6.4 all versions. FortiAnalyzer version 7.0.0 through 7.0.5 FortiAnalyzer version 7.0.6 and below, FortiAnalyzer version 7.2.0 through 7.2.1 FortiAnalyzer version 7.2.1 and below, FortiAnalyzer version 6.4.8 through 6.4.10 FortiAuthenticator 6.1 and 6.2 all versions FortiAuthenticator version 6.3.0 through 6.3.3 FortiAuthenticator version 6.4.0 through 6.4.1 FortiAuthenticator version 6.4.0 through 6.4.4 FortiClientMac version 6.0, 6.2 and 6.4 all versions FortiClientMac version 7.0.0 through 7.0.7 FortiClientWindows 6.0, 6.2 and 6.4 all versions FortiClientWindows version 6.0.0 through 6.0.10 FortiClientWindows version 6.2 all versions FortiClientWindows version 6.2.0 through 6.2.9 FortiClientWindows version 6.4 all versions FortiClientWindows version 6.4.0 through 6.4.9 FortiClientWindows version 7.0.0 through 7.0.7 FortiDDoS version 4.x, 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6 all versions FortiDDoS-F version 6.1.0 through 6.1.4 FortiDDoS-F version 6.2.0 through 6.2.2 FortiDDoS-F version 6.3.0 through 6.3.3 FortiDDoS-F version 6.4.0 FortiDeceptor 1.0, 1.1, 2.0, 2.1, 3.0, 3.1, 3.2 all versions FortiDeceptor version 3.3.0 through 3.3.3 FortiDeceptor version 4.0.0 through 4.0.2 FortiDeceptor version 4.1.0 FortiManager version 6.4.8 through 6.4.10	FortiManager version 7.0.0 through 7.0.5 FortiManager version 7.2.0 through 7.2.1 FortiNAC 8.7, 8.8, 9.1, 9.2 all versions FortiNAC version 9.4.0 through 9.4.1 FortiOS 6.2 all versions FortiOS all versions 6.2, 6.0 FortiOS version 6.2.0 through 6.2.12 FortiOS version 6.4.0 through 6.4.11 FortiOS version 6.4.0 through 6.4.12 FortiOS version 7.0.0 through 7.0.10 FortiOS version 7.0.0 through 7.0.9 FortiOS version 7.2.0 through 7.2.3 FortiProxy 1.0, 1.1, 1.2, 2.0 all versions FortiProxy all versions 2.0, 1.2, 1.1, 1.0 FortiProxy version 7.0.0 through 7.0.3 FortiProxy version 7.0.0 through 7.0.7 FortiProxy version 7.0.0 through 7.0.8 FortiProxy version 7.2.0 through 7.2.1 FortiProxy version 7.2.0 through 7.2.2 FortiSandbox 2.5,3.0, 3.1 all versions FortiSandbox version 3.0.1 through 3.0.7 FortiSandbox version 3.2.0 through 3.2.3 FortiSandbox version 4.0.0 through 4.0.2 FortiSandbox version 4.2.0 FortiSandbox version 4.2.0 through 4.2.2 FortiSIEM version 6.1.0 through 6.1.2 FortiSIEM version 6.2.0 through 6.2.1 FortiSIEM version 6.3.0 through 6.3.3 FortiSIEM version 6.4.0 FortiWeb 6.4 all versions FortiWeb version 6.0 all versions FortiWeb version 6.1 all versions FortiWeb version 6.2 all versions FortiWeb version 6.3.0 through 6.3.21 FortiWeb version 7.0.0 through 7.0.3 FortiSOAR version 6.4.5 or above FortiSOAR version 6.6.0 or above FortiSOAR version 7.0.4 or above FortiSOAR version 7.2.3 or above FortiSOAR version 7.3.2 or above FortiSOAR version 8.0.0 or above
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt?date=04-2023&severity=2,3,4

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-29186, CVE-2023-26458, CVE-2023-29187, CVE-2023-28761, CVE-2023-24528, CVE-2023-28763, CVE-2023-27499, CVE-2023-27897, CVE-2023-29189, CVE-2021-33683, CVE-2023-24527, CVE-2023-29185, CVE-2023-29108, CVE-2020-13936, CVE-2023-29109, CVE-2023-1903, CVE-2023-29110, CVE-2023-29112, CVE-2023-29111)
Description	SAP has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of these vulnerabilities could lead to Directory traversal, Information disclosure, Cross-site scripting, Code injection. SAP recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	ABAP Platform and SAP Web Dispatcher,Versions -WEBDISP 7.85, 7.89, KERNEL 7.85, 7.89, 7.91 SAP Application Interface Framework (Custom Hint of Message Dashboard Application,Versions – AIF 703, AIFX 702, S4CORE 100, 101, SAP_BASIS 755, 756, SAP_ABA 75C, 75D, 75E SAP Application Interface Framework (Log Message View of Message Dashboard),Versions – AIF 703, AIFX 702, S4CORE 101, SAP_BASIS 755, 756, SAP_ABA 75C, 75D, 75E SAP Application Interface Framework (Message Monitoring and Message Monitoring for Administrators Application, Versions – 600, 700 SAP Application Interface Framework (ODATA service),Versions – 755, 756 SAP Commerce, Versions – 1905, 2005, 2011 SAP CRM (WebClient UI),Versions – S4FND 102, 103, 104, 105, 106, 107, WEBCUIF, 700, 701, 731, 730, 746, 747, 748, 800, 801 SAP CRM, Versions – 700, 701, 702, 712, 713 SAP Fiori apps 1.0 for travel management in SAP ERP (My Travel Requests), Version -600 SAP GUI for HTML,Versions -KERNEL 7.22, 7.53, 7.547.77, 7.81, 7.85, 7.89, 7.91, KRNL64UC, 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT SAP HCM Fiori App My Forms (Fiori 2.0), Version – 605 SAP Landscape Management, Version – 3.0 SAP NetWeaver (BI CONT ADDON), Versions -707, 737, 747, 757 SAP NetWeaver AS for ABAP (Business Server Pages), Versions -700, 701, 702, 731, 740,750, 751, 752, 753, 754, 755, 756, 757 SAP NetWeaver AS for ABAP and ABAP Platform,Versions – 740, 750, 751, 752, 753, 754, 755, 756, 757, 791 SAP NetWeaver AS Java for Deploy Service, Version – 7.50 SAP NetWeaver Enterprise Portal,Version – 7.50 SAP Web Dispatcher and Internet Communication Manager, Versions -KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22,7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, KRNL64UC 7.21,7.21EXT, 7.22, 7.22EXT, 7.49, 7.53, 7.73, WEBDISP 7.53, 7.73, 7.77, 7.81, 7.82,7.83, KERNEL 7.21, 7.22,7.49, 7.53, 7.73, 7.77, 7.81, 7.82, 7.83 SapSetup (Software Installation Program), Version – 9.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=100

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2023-0482)
Description	IBM has released a security update addressing a privilege escalation vulnerability that exist in the IBM WebSphere Application Server Liberty. **CVE-2023-0482** – A vulnerability in the RESTEasy library used by IBM WebSphere Application Server Liberty when the feature restfulWS-3.0 or restfulWS-3.1 is enabled. Due to the creation of insecure temp files in the File.createTempFile() used in the DataSourceProvider, FileProvider and Mime4JWorkaround classes, RESTEasy could allow a local authenticated attacker to gain elevated privileges on the system by sending a specially-crafted request IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM WebSphere Application Server Liberty version 21.0.0.12 to 23.0.0.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6982895

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.