Advisory Alert

Alert Number: AAA20220419 **Date:** April 19, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
CISCO	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
Sonicwall	**High**	Post-Auth arbitrary file read Vulnerability
Citrix	**High**	Multiple Vulnerabilities
Juniper	**High**	Multiple Vulnerabilities
PaloAlto	**Medium**	Denial-of-Service Vulnerability

Description

Affected Product	CISCO
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-20695,CVE-2022-20739,CVE-2022-20716,CVE-2022-20692,CVE-2022-20714,CVE-2022-20697,CVE-2022-20681,CVE-2022-20761,CVE-2022-20661,CVE-2022-20731,CVE-2022-20684,CVE-2022-20683,CVE-2022-20682,CVE-2022-20678,CVE-2022-20622,CVE-2022-20693,CVE-2022-20735,CVE-2022-20747,CVE-2022-20717,CVE-2022-20679,CVE-2022-20677,CVE-2022-20718,CVE-2022-20719,CVE-2022-20694,CVE-2022-20676,CVE-2022-20758)
Description	Cisco has released security updates addressing multiple vulnerabilities which may lead attackers to cause Authentication Bypass, Denial of Service Vulnerability, Privilege Escalation Vulnerability, API Injection Vulnerability, Cross-Site Request Forgery. Cisco highly 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://tools.cisco.com/security/center/publicationListing.x

Affected Product	Microsoft	
Severity	**Critical**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-1125, CVE-2022-1127, CVE-2022-1128, CVE-2022-1129, CVE-2022-1130, CVE-2022-1131, CVE-2022-1133, CVE-2022-1134, CVE-2022-1135, CVE-2022-1136, CVE-2022-1137, CVE-2022-1138, CVE-2022-1139, CVE-2022-1143, CVE-2022-1145, CVE-2022-1146, CVE-2022-1232, CVE-2022-21983, CVE-2022-22008, CVE-2022-22009, CVE-2022-23257, CVE-2022-23259, CVE-2022-23268, CVE-2022-23292, CVE-2022-24472, CVE-2022-24473, CVE-2022-24475, CVE-2022-24482, CVE-2022-24483, CVE-2022-24485, CVE-2022-24487, CVE-2022-24490, CVE-2022-24491, CVE-2022-24492, CVE-2022-24493,CVE-2022-24495, CVE-2022-24497, CVE-2022-24498, CVE-2022-24500, CVE-2022-24523, CVE-2022-24527, CVE-2022-24528, CVE-2022-24532, CVE-2022-24533, CVE-2022-24534, CVE-2022-24536, CVE-2022-24537, CVE-2022-24539, CVE-2022-24540, CVE-2022-24541, CVE-2022-24543, CVE-2022-24545, CVE-2022-24765, CVE-2022-24767, CVE-2022-26783, CVE-2022-26785, CVE-2022-26807, CVE-2022-26808, CVE-2022-26809, CVE-2022-26811, CVE-2022-26812, CVE-2022-26813, CVE-2022-26814, CVE-2022-26815, CVE-2022-26816, CVE-2022-26817, CVE-2022-26818, CVE-2022-26819, CVE-2022-26820, CVE-2022-26821, CVE-2022-26822, CVE-2022-26823, CVE-2022-26824, CVE-2022-26825, CVE-2022-26826, CVE-2022-26827, CVE-2022-26828, CVE-2022-26829, CVE-2022-26830, CVE-2022-26891, CVE-2022-26894, CVE-2022-26895, CVE-2022-26896, CVE-2022-26897, CVE-2022-26898, CVE-2022-26900, CVE-2022-26901, CVE-2022-26903, CVE-2022-26904, CVE-2022-26907, CVE-2022-26908, CVE-2022-26909, CVE-2022-26910, CVE-2022-26911, CVE-2022-26912, CVE-2022-26916, CVE-2022-26917, CVE-2022-26918, CVE-2022-26919, CVE-2022-26920, CVE-2022-26924)	
Description	Microsoft has issued Security Updates to address a number of vulnerabilities in a 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 Framework Active Directory Domain Services Azure SDK Azure Site Recovery LDAP - Lightweight Directory Access Protocol Microsoft Bluetooth Driver Microsoft Dynamics Microsoft Edge (Chromium-based) Microsoft Graphics Component Microsoft Local Security Authority Server (lsasrv) Microsoft Office Excel Microsoft Office SharePoint Microsoft Windows ALPC Microsoft Windows Codecs Library Microsoft Windows Media Foundation Power BI Role: DNS Server Role: Windows Hyper-V Skype for Business Visual Studio Visual Studio Code Windows Ancillary Function Driver for WinSock Windows App Store Windows AppX Package Manager Windows Cluster Client Failover Windows Cluster Shared Volume (CSV) Windows Common Log File System Driver Windows Defender	Windows DWM Core Library Windows Endpoint Configuration Manager Windows Fax Compose Form Windows Feedback Hub Windows File Explorer Windows File Server Windows Installer Windows iSCSI Target Service Windows Kerberos Windows Kernel Windows Local Security Authority Subsystem Service Windows Media Windows Network File System Windows PowerShell Windows Print Spooler Components Windows RDP Windows Remote Procedure Call Runtime Windows schannel Windows SMB Windows Telephony Server Windows Upgrade Assistant Windows User Profile Service Windows Win32K Windows Work Folder Service YARP reverse proxy
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2022-Apr	

Affected Product	Sonicwall
Severity	**High**
Affected Vulnerability	Post-Auth arbitrary file read Vulnerability (CVE-2022-22279)
Description	SonicWall has identified 'Post Authentication Arbitrary File Read' vulnerability impacting end-of-life Secure Remote Access (SRA) series products, specifically appliances running all 8.x or 9.0.0.5-19sv and earlier versions. And Secure Mobile Access (SMA) 100 series products running old firmware 9.0.0.9-26sv and earlier versions.
Affected Products	SRA Series 9.0.0.5-19sv and earlier versions. SMA100 Series 9.0.0.9-26sv and earlier versions.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0006

Affected Product	Citrix
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-27505, CVE-2022-27506, CVE-2022-21827)
Description	Citrix has released security updates addressing multiple vulnerabilities which may lead attackers to cause Reflected cross site scripting, Use of Hard-coded credentials, improper access control Citrix highly recommends to apply necessary workarounds at earliest to avoid issues.
Affected Products	Citrix SD-WAN Standard/Premium Edition Appliance before 11.4.3a Citrix SD-WAN Center Management Console versions before 11.4.3 Citrix SD-WAN Standard/Premium Edition Appliance versions before 11.4.1 Citrix SD-WAN Orchestrator for On-Premises versions before 13.2.1 Citrix Gateway Plug-in for Windows versions before 21.9.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX370550 https://support.citrix.com/article/CTX341455

Affected Product	Juniper
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-22186, CVE-2022-22190, CVE-2022-22198, CVE-2022-22188, CVE-2022-22194, CVE-2021-4034, CVE-2022-22185, CVE-2022-22187, CVE-2022-22182, CVE-2022-22183, CVE-2022-22181, CVE-2022-22197, CVE-2022-22195)
Description	Juniper has released security patch updates addressing multiple vulnerabilities that exists in multiple juniper products. An attacker could use these vulnerabilities to gain access to systems and perform malicious activities. Most of the vulnerabilities are found in the Junos OS. It is highly recommended to apply necessary fixes at earliest to the Juniper products to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/global-search/%40uri?language=en_US#sort=date%20descending&f:ctype=[Security%20Advisories]&f:slevel=[Critical,High]

Affected Product	PaloAlto
Severity	**Medium**
Affected Vulnerability	Denial-of-Service Vulnerability (CVE-2022-0023)
Description	Improper handling of exceptional conditions vulnerability that exists in the DNS proxy feature of Palo Alto Networks PAN-OS software leads to a meddler-in-the-middle (MITM) to send specifically crafted traffic to the firewall causing the service to restart unexpectedly. Multiple attempts to send this request leads to a denial-of-service to all PAN-OS services by restarting the device in maintenance mode.
Affected Products	PAN-OS 8.1 versions earlier than PAN-OS 8.1.22; PAN-OS 9.0 versions earlier than PAN-OS 9.0.16; PAN-OS 9.1 versions earlier than PAN-OS 9.1.13; PAN-OS 10.0 versions earlier than PAN-OS 10.0.10; PAN-OS 10.1 versions earlier than PAN-OS 10.1.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2022-0023

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.