Advisory Alert

Alert Number: AAA20210826 **Date:** August 26, 2021

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-1577, CVE-2021-1587, CVE-2021-1588, CVE-2021-1586, CVE-2021-1523, CVE-2021-1578, CVE-2021-1579, CVE-2021-1592, CVE-2021-1590, CVE-2021-1591, CVE-2021-1584, CVE-2021-1583, CVE-2021-1582, CVE-2021-1580, CVE-2021-1581, CVE-2019-1727)
Description	Cisco has released updates addressing multiple vulnerabilities that exists in their products such as Arbitrary File Read and Write Vulnerability, Denial of Service Vulnerability, Privilege Escalation Vulnerability, Access Control List Bypass Vulnerability, Arbitrary File Read Vulnerability, Cross-Site Scripting Vulnerability, Command Injection and File Upload Vulnerabilities. Cisco highly recommends to apply necessary security fixes to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-frw-Nt3RYxR2 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ngoam-dos-LTDb9Hv https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-mpls-oam-dos-sGO9x5GM https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n9kaci-tcp-dos-YXukt6gM https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n9kaci-queue-wedge-cLDDEfKF https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-pesc-pkmGK4J https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-chvul-CKfGYBh8 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-ssh-dos-MgvmyrQy https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-login-blockfor-RwjGVEcu https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nexus-acl-vrvQYPVe https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-naci-mdvul-vrKVgNU https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-naci-afr-UtjfO2D7 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-scss-bFT75YrM https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-mdvul-HBsJBuvW https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-nxos-pyth-escal

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)
Description	Microsoft has released updates addressing multiple vulnerabilities that exists in Microsoft Exchange server such as Remote Code Execution Vulnerability, Elevation of Privilege Vulnerability, Security Feature Bypass Vulnerability. Malicious attackers are using the ProxyShell chain of vulnerabilities to install at least five different web shells to Microsoft Exchange servers. These separate vulnerabilities can be exploited through a transmission control protocol port 445 to execute arbitrary commands on Exchange servers, without authentication. Failure to patch could put the servers at risk of ransomware attacks. Microsoft highly recommends to apply necessary security fixes to avoid issues.
Affected Products	Microsoft Exchange Server 2013 Microsoft Exchange Server 2016 Microsoft Exchange Server 2019
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34523 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31207

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.