Advisory Alert

Alert Number: AAA20220309 **Date:** March 9, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	**Multiple Vulnerabilities**
Citrix	**Low**	Information disclosure

Description

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-8927, CVE-2022-0789, CVE-2022-0790, CVE-2022-0791, CVE-2022-0792, CVE-2022-0793, CVE-2022-0794, CVE-2022-0795, CVE-2022-0796, CVE-2022-0797, CVE-2022-0798, CVE-2022-0799, CVE-2022-0800, CVE-2022-0801, CVE-2022-0802, CVE-2022-0803, CVE-2022-0804, CVE-2022-0805, CVE-2022-0806, CVE-2022-0807, CVE-2022-0808, CVE-2022-0809, CVE-2022-21967, CVE-2022-21975, CVE-2022-21977, CVE-2022-21990, CVE-2022-22006, CVE-2022-22007, CVE-2022-22010, CVE-2022-23265, CVE-2022-23266, CVE-2022-23277, CVE-2022-23278, CVE-2022-23281, CVE-2022-23282, CVE-2022-23283, CVE-2022-23285, CVE-2022-23286, CVE-2022-23287, CVE-2022-23288, CVE-2022-23294, CVE-2022-23295, CVE-2022-23297, CVE-2022-23298, CVE-2022-23299, CVE-2022-23300, CVE-2022-23301, CVE-2022-24451, CVE-2022-24452, CVE-2022-24453, CVE-2022-24456, CVE-2022-24457, CVE-2022-24460, CVE-2022-24461, CVE-2022-24462, CVE-2022-24463, CVE-2022-24465, CVE-2022-24467, CVE-2022-24468, CVE-2022-24469, CVE-2022-24470, CVE-2022-24471, CVE-2022-24501, CVE-2022-24502, CVE-2022-24503, CVE-2022-24505, CVE-2022-24506, CVE-2022-24508, CVE-2022-24509, CVE-2022-24510, CVE-2022-24511, CVE-2022-24512, CVE-2022-24515, CVE-2022-24517, CVE-2022-24518, CVE-2022-24519, CVE-2022-24520, CVE-2022-24522, CVE-2022-24525, CVE-2022-24526)
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 that necessary security fixes be applied as soon as possible to avoid problems.
Affected Products	.NET and Visual Studio Azure Site Recovery Microsoft Defender for Endpoint Microsoft Defender for IoT Microsoft Edge (Chromium-based) Microsoft Exchange Server Microsoft Intune Microsoft Office Visio Microsoft Office Word Microsoft Windows ALPC Microsoft Windows Codecs Library Paint 3D Role: Windows Hyper-V Skype Extension for Chrome Tablet Windows User Interface Visual Studio Code Windows Ancillary Function Driver for WinSock Windows CD-ROM Driver Windows Cloud Files Mini Filter Driver Windows COM Windows Common Log File System Driver Windows DWM Core Library Windows Event Tracing Windows Fastfat Driver Windows Fax and Scan Service Windows HTML Platform Windows Installer Windows Kernel Windows Media Windows PDEV Windows Point-to-Point Tunneling Protocol Windows Print Spooler Components Windows Remote Desktop Windows Security Support Provider Interface Windows SMB Server Windows Update Stack XBox
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2022-Mar

Affected Product	Citrix
Severity	**Low**
Affected Vulnerability	Information disclosure (CVE-2022-26355)
Description	Citrix Federated Authentication Service (FAS) has an issue that causes deployments set to store a registration authority certificate's private key in a Trusted Platform Module (TPM) to store that key incorrectly in the Microsoft Software Key Storage Provider (MSKSP). This problem only arises if PowerShell was used when configuring FAS to store the registration authority certificate's private key in the TPM. It does not happen if the TPM was not selected for use or if the FAS administration console was used for configuration.
Affected Products	Citrix Virtual Apps and Desktops
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX341587

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.