Advisory Alert

Alert Number: AAA20220209 **Date:** February 9, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
Citrix	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-0452, CVE-2022-0453, CVE-2022-0454, CVE-2022-0455, CVE-2022-0456, CVE-2022-0457, CVE-2022-0458, CVE-2022-0459, CVE-2022-0460, CVE-2022-0461, CVE-2022-0462, CVE-2022-0463, CVE-2022-0464, CVE-2022-0465, CVE-2022-0466, CVE-2022-0467, CVE-2022-0468, CVE-2022-0469, CVE-2022-0470, CVE-2022-21844, CVE-2022-21926, CVE-2022-21927, CVE-2022-21965, CVE-2022-21968, CVE-2022-21971, CVE-2022-21974, CVE-2022-21984, CVE-2022-21985, CVE-2022-21986, CVE-2022-21987, CVE-2022-21988, CVE-2022-21989, CVE-2022-21991, CVE-2022-21992, CVE-2022-21993, CVE-2022-21995, CVE-2022-21997, CVE-2022-21998, CVE-2022-22003, CVE-2022-22004, CVE-2022-22005, CVE-2022-22709, CVE-2022-22712, CVE-2022-22716, CVE-2022-22717, CVE-2022-23252, CVE-2022-23254, CVE-2022-23255, CVE-2022-23256, CVE-2022-23261, CVE-2022-23262, CVE-2022-23263, CVE-2022-23269, CVE-2022-23272, CVE-2022-23274, CVE-2022-23276, CVE-2022-23280)
Description	Microsoft has released its February 2022 Security Updates which address multiple vulnerabilities across several products, which an attacker could use to gain control of an affected system. Microsoft highly recommends applying relevant patches at the earliest to avoid issues.
Affected Products	• Azure Data Explorer • Kestrel Web Server • Microsoft Dynamics • Microsoft Dynamics GP • Microsoft Edge (Chromium-based) • Microsoft Office • Microsoft Office Excel • Microsoft Office Outlook • Microsoft Office SharePoint • Microsoft Office Visio • Microsoft OneDrive • Microsoft Teams • Microsoft Windows Codecs Library • Power BI • Roaming Security Rights Management Services • Role: DNS Server • Role: Windows Hyper-V • SQL Server • Visual Studio Code • Windows Common Log File System Driver • Windows DWM Core Library • Windows Kernel • Windows Kernel-Mode Drivers • Windows Named Pipe File System • Windows Print Spooler Components • Windows Remote Access Connection Manager • Windows Remote Procedure Call Runtime • Windows User Account Profile • Windows Win32K
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2022-Feb

Affected Product	**Citrix**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-23034, CVE-2022-23035, CVE-2021-0145)
Description	Citrix has released security updates for Citrix Hypervisor to address several vulnerabilities. Successful exploitation of these flaws may allow privileged code in a guest VM to cause the host to crash.
Affected Products	Citrix Hypervisor
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX337526

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.