Advisory Alert

Alert Number: AAA20210512 **Date:** May 12, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	**Multiple Vulnerabilities**
Citrix	**High**	Local privilege escalation
VMware	**Low**	Cross-site scripting vulnerability

Description

Affected Product	**Microsoft**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities ((CVE-2020-24587,CVE-2021-1720,CVE-2021-26419,CVE-2021-28455,CVE-2021-28465,CVE-2021-28474,CVE-2021-28479,CVE-2021-31166,CVE-2021-31171,CVE-2021-31173,CVE-2021-31174,CVE-2021-31175,CVE-2021-31176,CVE-2021-31177,CVE-2021-31178,CVE-2021-31179,CVE-2021-31180,CVE-2021-31184,CVE-2021-31186,CVE-2021-31191,CVE-2021-31205,CVE-2021-31206,CVE-2021-31207,CVE-2021-31209,CVE-2021-31211,CVE-2021-31213,CVE-2021-31214,CVE-2021-31936)
Description	Microsoft has released Security Updates addressing multiple vulnerabilities that exists with multiple Microsoft products. The most severe could allow a remote attacker to take control of an affected system. It is highly recommended by Microsoft to apply necessary security fixes at earliest to avoid issues.
Affected Products	.NET Core & Visual Studio HTTP.sys Internet Explorer Microsoft Accessibility Insights for Web Microsoft Bluetooth Driver Microsoft Dynamics Finance & Operations Microsoft Exchange Server Microsoft Graphics Component Microsoft Office Microsoft Office Access Microsoft Office Excel Microsoft Office SharePoint Microsoft Office Word Microsoft Windows Codecs Library Microsoft Windows IrDA Open Source Software Role: Hyper-V Skype for Business and Microsoft Lync Visual Studio Visual Studio Code Windows Container Isolation FS Filter Driver Windows Container Manager Service Windows Cryptographic Services Windows CSC Service Windows Desktop Bridge Windows OLE Windows Projected File System FS Filter Windows RDP Client Windows SMB Windows SSDP Service Windows WalletService Windows Wireless Networking
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2021-May

Affected Product	Citrix
Severity	**High**
Affected Vulnerability	Local privilege escalation (CVE-2021-22907)
Description	Citrix has released security updates addressing local privilege escalation vulnerability that exists in Citrix workspace app. Successful exploitation of this flaw could lead a local attacker to escalate their privilege level to “SYSTEM” on the computer that runs Citrix workspace app for windows.
Affected Products	Citrix workspace app
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX307794

Affected Product	VMware
Severity	**Low**
Affected Vulnerability	Cross-site scripting vulnerability (CVE-2021-21990)
Description	VMware has released Security Updates addressing cross-site scripting vulnerability which occurs as a result of not validating the incoming requests during device enrollment by VMware workspace ONE UEM. By exploiting this flaw a malicious attacker could inject code or redirect the user to another site during enrollment process. VMware highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	VMware Workspace ONE UEM console (Version 1912, 2001, 2003, 2004, 2005, 2006, 2007, 2008, 2010, 2011, 2101, 2102)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2021-0008.html

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.