TLP: WHITE

Advisory Alert

Alert Number: AAA20211013 **Date:** October 13, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	**Multiple Vulnerabilities**
LibreOffice	**Critical**	**Multiple Vulnerabilities**
VMware	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-1971, CVE-2021-26427, CVE-2021-26441, CVE-2021-3449, CVE-2021-3450, CVE-2021-37974, CVE-2021-37975, CVE-2021-37976, CVE-2021-38662, CVE-2021-38663, CVE-2021-38672, CVE-2021-40454, CVE-2021-40456, CVE-2021-40457, CVE-2021-40460, CVE-2021-40468, CVE-2021-40469, CVE-2021-40471, CVE-2021-40472, CVE-2021-40473, CVE-2021-40474, CVE-2021-40475, CVE-2021-40479, CVE-2021-40480, CVE-2021-40481, CVE-2021-40482, CVE-2021-40485, CVE-2021-40486, CVE-2021-40487, CVE-2021-40489, CVE-2021-41332, CVE-2021-41336, CVE-2021-41337, CVE-2021-41342, CVE-2021-41343, CVE-2021-41352, CVE-2021-41355, CVE-2021-41361, CVE-2021-41363)
Description	Microsoft has released Security Updates addressing multiple vulnerabilities that exists with multiple Microsoft products, features and roles. In addition to security changes for the vulnerabilities, updates include defense-in-depth updates to help improve security-related features. It is highly recommended by Microsoft to apply necessary security fixes at earliest to avoid issues.
Affected Products	.NET Core & Visual Studio Active Directory Federation Services Console Window Host HTTP.sys Microsoft DWM Core Library Microsoft Dynamics Microsoft Edge (Chromium-based) Microsoft Exchange Server Microsoft Graphics Component Microsoft Intune Microsoft Office Excel Visual Studio Windows AppContainer Windows AppX Deployment Service Windows Bind Filter Driver Windows Cloud Files Mini Filter Driver Windows Common Log File System Driver Windows Desktop Bridge Microsoft Office SharePoint Microsoft Office Visio Microsoft Office Word Microsoft Windows Codecs Library Rich Text Edit Control Role: DNS Server Role: Windows Active Directory Server Role: Windows AD FS Server Role: Windows Hyper-V System Center Windows DirectX Windows Event Tracing Windows exFAT File System Windows Fastfat Driver Windows Installer Windows Kernel Windows MSHTML Platform Windows Nearby Sharing Windows Network Address Translation (NAT) Windows Print Spooler Components Windows Remote Procedure Call Runtime Windows Storage Spaces Controller Windows TCP/IP Windows Text Shaping Windows Win32K
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2021-Oct

Affected Product	**LibreOffice**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-25634, CVE-2021-25633, CVE-2021-25635)
Description	LibreOffice has released Security Updates addressing multiple vulnerabilities including timestamp manipulation with signature wrapping, content manipulation with double certificate, content manipulation with certificate validation that exists in their products which leads attackers to perform malicious activities to alter documents to make them appear as if they are digitally signed by a trusted source. LibreOffice highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	prior to update LibreOffice 7.0.6/7.1.2 and 7.0.5/7.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.libreoffice.org/about-us/security/advisories/cve-2021-25634/ https://www.libreoffice.org/about-us/security/advisories/cve-2021-25633/ https://www.libreoffice.org/about-us/security/advisories/cve-2021-25635/

Affected Product	VMware
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-22033, CVE-2021-22035, CVE-2021-22036)
Description	VMware has released Security Updates addressing multiple vulnerabilities including server side request forgery, CSV injection, and open redirect vulnerability that contains in their products which leads attackers to perform malicious activities. VMware highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	VMware vRealize Operations VMware vRealize Log Insight VMware vRealize Orchestrator VMware Cloud Foundation vRealize Suite Lifecycle Manager
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2021-0023.html https://www.vmware.com/security/advisories/VMSA-2021-0022.html https://www.vmware.com/security/advisories/VMSA-2021-0021.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.