Advisory Alert

Alert Number: AAA20211110 **Date:** November 10, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
Citrix	**Critical**	Multiple Vulnerabilities
Samba	**High**	Multiple Vulnerabilities

Description

Affected Product	**Microsoft**	
Severity	**Critical**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-26443,CVE-2021-26444,CVE-2021-3711,CVE-2021-38631,CVE-2021-38665,CVE-2021-38666,CVE-2021-40442,CVE-2021-41368,CVE-2021-41371,CVE-2021-41373,CVE-2021-41374,CVE-2021-41375,CVE-2021-41376,CVE-2021-41379,CVE-2021-42275,CVE-2021-42277,CVE-2021-42278,CVE-2021-42280,CVE-2021-42282,CVE-2021-42284,CVE-2021-42287,CVE-2021-42291,CVE-2021-42292,CVE-2021-42296,CVE-2021-42298,CVE-2021-42300,CVE-2021-42301,CVE-2021-42302,CVE-2021-42303,CVE-2021-42304,CVE-2021-42321,CVE-2021-42323,CVE-2021-43208,CVE-2021-43209)	
Description	Microsoft has released its November 2021 Security Updates which address multiple vulnerabilities across several of products, which an attacker could use to gain control of an affected system. Microsoft highly recommends to apply relevant patches at earliest to avoid issues.	
Affected Products	3D Viewer Azure Azure RTOS Azure Sphere Microsoft Dynamics Microsoft Edge (Chromium-based) Microsoft Edge (Chromium-based) in IE Mode Microsoft Exchange Server Microsoft Office Microsoft Office Access Microsoft Office Excel Microsoft Office SharePoint Microsoft Office Word Microsoft Windows Microsoft Windows Codecs Library Power BI Role: Windows Hyper-V Visual Studio	Visual Studio Code Windows Active Directory Windows COM Windows Core Shell Windows Cred SSProvider Protocol Windows Defender Windows Desktop Bridge Windows Diagnostic Hub Windows Fastfat Driver Windows Feedback Hub Windows Hello Windows Installer Windows Kernel Windows NTFS Windows RDP Windows Scripting Windows Virtual Machine Bus
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2021-Nov	

Affected Product	**Citrix**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-22955, CVE-2021-22956)
Description	Citrix has released Security Updates addressing multiple vulnerabilities that exists with Citrix products. **CVE-2021-22955 -** Unauthenticated denial of service **CVE-2021-22956 -** Temporary disruption of the Management GUI, Nitro API and RPC communication
Affected Products	Citrix ADC, Citrix Gateway Citrix ADC, Citrix Gateway Citrix SD-WAN WANOP Edition
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX330728

Affected Product	**Samba**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2016-2124, CVE-2020-25717, CVE-2020-25718, CVE-2020-25719, CVE-2020-25721, CVE-2020-25722, CVE-2021-3738, CVE-2021-23192)
Description	Samba released security updates to address vulnerabilities in multiple versions of Samba. **CVE-2016-2124 -** Even if Kerberos authentication was requested by the user or application, a man in the middle attack can force the client side SMB1 code to fall back to plaintext or NTLM based authentication. **CVE-2020-25717 -** Samba might inadvertently assign domain users to local users. **CVE-2020-25718 -** When a RODC joined the Samba AD DC, the RODC did not validate whether the RODC was allowed to print a ticket for that user. **CVE-2020-25719 -** If the Samba AD DC did not strictly require a Kerberos PAC and always utilized the SIDs contained within, it may become confused about which user a ticket represented. The result might be a complete domain compromise. **CVE-2020-25721 -** Linux applications can now obtain a reliable SID (and samAccountName) in issued tickets using Samba as an AD DC. **CVE-2020-25722 -** Per-attribute and schema-based permission checks were not correctly implemented at several points in the Samba AD DC, allowing to total domain compromise. **CVE-2021-3738 -** When a sub-connection is closed, the AD DC RPC server can use memory that was free()ed. **CVE-2021-23192 -** An attacker may replace later fragments with their own data, bypassing the signature requirements, if a client to a Samba server sent a very large DCE/RPC request and chose to fragment it.
Affected Products	Samba 3.0.0 to 4.15.1 All Samba versions since Samba 3.0c Samba 4.0.0 and later
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.samba.org/samba/history/security.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