Advisory Alert

Alert Number: AAA20210609 **Date:** June 9, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	Microsoft
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-26414,CVE-2021-31199,CVE-2021-31201,CVE-2021-31938,CVE-2021-31939,CVE-2021-31940,CVE-2021-31941,CVE-2021-31942,CVE-2021-31943,CVE-2021-31944,CVE-2021-31945,CVE-2021-31946,CVE-2021-31949,CVE-2021-31955,CVE-2021-31956,CVE-2021-31958,CVE-2021-31959,CVE-2021-31960,CVE-2021-31962,CVE-2021-31965,CVE-2021-31967,CVE-2021-31971,CVE-2021-31972,CVE-2021-31975,CVE-2021-31976,CVE-2021-31977,CVE-2021-31978,CVE-2021-31980,CVE-2021-31983,CVE-2021-31985,CVE-2021-33739,CVE-2021-33741,CVE-2021-33742)
Description	Microsoft has released security updates addressing multiple vulnerabilities that exists in their products. The most severe could cause privilege escalation, remote code execution, memory corruption, security by pass and denial of service. Microsoft highly recommends to apply necessary security fixes to avoid issues.
Affected Products	.NET Core & Visual Studio 3D Viewer Microsoft DWM Core Library Microsoft Intune Microsoft Office Microsoft Office Excel Microsoft Office Outlook Microsoft Office SharePoint Microsoft Scripting Engine Microsoft Windows Codecs Library Paint 3D Role: Hyper-V Visual Studio Code - Kubernetes Tools Windows Bind Filter Driver Windows Common Log File System Driver Windows Cryptographic Services Windows DCOM Server Windows Defender Windows Drivers Windows Event Logging Service Windows Filter Manager Windows HTML Platform Windows Installer Windows Kerberos Windows Kernel Windows Kernel-Mode Drivers Windows Network File System Windows NTFS Windows NTLM Windows Print Spooler Components Windows Remote Desktop Windows TCP/IP
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2021-Jun

Affected Product	Intel
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-12357,CVE-2020-8670,CVE-2020-8700,CVE-2020-12359,CVE-2020-12358,CVE-2021-0095,CVE-2020-12360,CVE-2020-24486,CVE-2020-24513,CVE-2021-0133,CVE-2021-0132,CVE-2021-0131,CVE-2021-0134,CVE-2021-0100,CVE-2021-0106,CVE-2021-0104)
Description	Intel has released security updates addressing multiple vulnerabilities that exists in their products. The most severe could cause privilege escalation and denial of service on Intel products. It is highly recommended by Intel to apply necessary security fixes to avoid issues.
Affected Products	Multiple Intel products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00463.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00465.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00521.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00537.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00541.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00545.html

Affected Product	Citrix
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-8299,CVE-2020-8300)
Description	Citrix has released security updates addressing multiple vulnerabilities that exists in their products. CVE-2020-8299 - Successful exploitation of this flaw could cause a network based denial of service in Layer 2 network segment. CVE-2020-8300 - Successful exploitation of this flaw could cause SAML authentication hijack through a phishing attack to steal a valid user session It is highly recommended by Citrix to apply necessary security fixes to avoid issues.
Affected Products	Citrix ADC and Citrix Gateway 13.0 before 13.0-76.29 Citrix ADC and Citrix Gateway 12.1 before 12.1-61.18 Citrix ADC and NetScaler Gateway 11.1 before 65.20 Citrix ADC 12.1-FIPS before 12.1-55.238 Citrix SD-WAN WANOP 11.4 before 11.4.0 Citrix SD-WAN WANOP 11.3 before 11.3.2 Citrix SD-WAN WANOP 11.3 before 11.3.1a Citrix SD-WAN WANOP 11.2 before 11.2.3a Citrix SD-WAN WANOP 11.1 before 11.1.2c Citrix SD-WAN WANOP 10.2 before 10.2.9a Citrix ADC and Citrix Gateway 13.0. before 13.0-82.41 Citrix ADC and Citrix Gateway 12.1 before 12.1-62.23 Citrix ADC and NetScaler Gateway 11.1 before 11.1-65.20 Citrix ADC 12.1-FIPS before 12.1-55.238
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX297155

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.