Vulnerability in various Products for October 11-20, 2021, as informed by CERT-In for necessary actions

Detailed Vulnerability Note may be seen from CERT-In Website

https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2021-XXXX, substituting XXXX with the number in second column

Kindly confirm action taken by your organisation.

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
1	CIVN-2021-0256	Google Chrome versions prior to 94.0.4606.81.	Multiple vulnerabilities have been reported in Google Chrome which could be exploited by an attacker to compromise a targeted system.	High	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop.html
5	CIVN-2021-0260	•Microsoft Windows Server 2019 •Microsoft Windows 10 1809 for x64-based Systems •Microsoft Windows 10 2004 for x64-based Systems •Microsoft Windows 10 1909 for ARM64-based Systems •Microsoft Windows 10 20H2 for x64-based Systems •Microsoft Windows Server (Server Core installation) 2019 •Microsoft Windows Server (Server Core installation) 2004 •Microsoft Windows Server (Server Core installation) 20H2 •Microsoft Windows 10 21H1 for x64-based Systems	A vulnerability has been reported in Microsoft Windows Hyper-V which could allow a remote attacker to execute arbitrary code on the targeted system.	High	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40461 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38672

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Microsoft Windows Server (Server Core installation) 2022 •Microsoft Windows 11 x64 •Microsoft Windows Server 2022			
8	CIVN-2021-0263	•Windows Server 2012 R2 (Server Core installation) •Windows Server 2012 (Server Core installation) •Windows Server 2008 •Windows Server 2008 R2 for x64-based Systems •Windows Server 2008 for 32-bit Systems •Windows Server 2016 •Windows 7 for x64-based Systems •Windows 7 for 32-bit Systems •Windows RT 8.1 •Windows 8.1 for x64-based systems •Windows 8.1 for 32-bit systems •Windows 10 Version 1607 for x64-based Systems •Windows 10 Version 1607 for 32-bit Systems •Windows 10 for x64-based Systems •Windows 10 for 32-bit Systems •Windows 11 for ARM64-based Systems •Windows 11 for x64-based Systems •Windows Server, version 20H2 •Windows 10 Version 20H2 •Windows Server, version 2004 •Windows 10 Version 2004 •Windows Server 2022 (Server Core installation)	An Elevation of Privilege vulnerability has been reported in Microsoft WindowsWin32kwhich could allow an attacker to obtain elevated privileges on the targeted system.	High	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-40449

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows 10 Version 21H1 •Windows 10 Version 1909 •Windows Server 2019 (Server Core installation) •Windows 10 Version 1809 for ARM64-based Systems •Windows 10 Version 1809 for x64-based Systems •Windows 10 Version 1809 for 32-bit Systems			
9	CIVN-2021-0264	•Acrobat DC and Acrobat Reader DC (Continuous) versions 21.007.20095 and prior for Windows •Acrobat DC and Acrobat Reader DC (Continuous) versions 21.007.20096 and prior for macOS •Acrobat 2020 and Acrobat Reader 2020 (Classic 2020) versions 20.004.30015 and prior for Windows & macOS •Acrobat 2017 and Acrobat Reader 2017 (Classic 2017) versions 17.011.30202 and prior for Windows & macOS	Multiple vulnerabilities have been reported in Acrobat DC and Acrobat Reader DC, which could allow an attacker to execute arbitrary code, gain escalated privileges on the targeted system.	High	https://helpx.adobe.com/security/products/acrobat/apsb21-104.html
15	CIAD-2021-0041	•Windows •Microsoft Office •Developer Tools •System Center •Browser •Microsoft Dynamics •.NET 5.0 •Intune management extension	Multiple vulnerabilities have been reported in various Microsoft products, which could be exploited by an attacker to access sensitive information, bypass security restrictions, perform a denial of service (DoS) attack, escalating privileges, perform Spoofing attacks or executing arbitrary codes on the targeted system.	High	https://msrc.microsoft.com/update-guide/releaseNote/2021-Oct