Vulnerability in various Products for January 01-10, 2022, 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-2022-XXXX, substituting XXXX with the number in second column

Please update the below mentioned applications/window's version to latest version to avoid security risks. Kindly confirm action taken in your organisation.

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
2	CIVN-2022-0002	Multiple Vulnerabilities in Google Chrome •Google Chrome versions prior to 97.0.4692.71.	Multiple vulnerabilities have been reported in Google Chrome which could be exploited by a remote attacker to execute arbitrary code on the targeted system.	HIGH	Update to Google Chrome version 97.0.4692.71. https://chromereleases.googleblog.com/2022/01/stable-channel-update-for-desktop.html
7	CIVN-2022-0007	Multiple Vulnerabilities in Adobe Acrobat and Reader •Acrobat DC (Continuous) versions 21.007.20099 and prior for Windows and MacOS •Acrobat Reader DC (Continuous) versions 21.007.20099 and prior for Windows and macOS •Acrobat 2020 (Classic 2020) versions 20.004.30017 and prior for Windows & macOS •Acrobat Reader 2020 (Classic 2020) versions 20.004.30017 and prior for Windows & macOS	Multiple vulnerabilities have been reported in Adobe Acrobat and Adobe Acrobat Reader, which could allow an attacker to execute arbitrary code, cause memory leak, cause	HIGH	Apply appropriate patches as mentioned in the Adobe Security Bulletin https://helpx.adobe.com/security/products/acrobat/apsb22-

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Acrobat 2017 (Classic 2017) versions 17.011.30204 and prior for Windows & macOS •Acrobat Reader 2017 (Classic 2017) versions 17.011.30204 and prior for Windows & macOS	application denial of service, bypass security features and escalate privileges on the targeted system.		01.html
8	CIVN-2022-0008	Remote code execution vulnerability in Microsoft Office •Microsoft SharePoint Foundation 2013 Service Pack 1 •Microsoft SharePoint Foundation 2013 Service Pack 1 •Microsoft Office Web Apps Server 2013 Service Pack 1 •Microsoft Office 2013 Service Pack 1 (64-bit editions) •Microsoft Office 2013 Service Pack 1 (64-bit editions) •Microsoft Office 2013 Service Pack 1 (64-bit editions) •Microsoft Office 2013 Service Pack 1 (32-bit editions) •Microsoft Office 2013 Service Pack 1 (32-bit editions) •Microsoft Office 2013 Service Pack 1 (32-bit editions) •Microsoft Office 2013 RT Service Pack 1 •Microsoft Office 2013 RT Service Pack 1 •Microsoft Office 2013 RT Service Pack 1 •Microsoft Excel 2013 Service Pack 1 (64-bit editions) •Microsoft Excel 2013 Service Pack 1 (32-bit editions) •Microsoft Excel 2013 RT Service Pack 1 •Microsoft Office 2016 (64-bit edition) •Microsoft Office 2016 (64-bit edition) •Microsoft Office 2016 (64-bit edition) •Microsoft Office 2016 (32-bit edition) •Microsoft Office 2016 (32-bit edition) •Microsoft Office 2016 (32-bit edition) •Microsoft Excel 2016 (64-bit edition) •Microsoft Excel 2016 (32-bit edition)	A vulnerability has been reported in Microsoft Office which could allow a remote attacker to execute arbitrary code on a targeted system.	HIGH	Apply appropriate patches as mentioned by the vendor https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21840

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•SharePoint Server Subscription Edition Language Pack •Microsoft SharePoint Server Subscription Edition •Microsoft Office LTSC 2021 for 32-bit editions •Microsoft Office LTSC 2021 for 64-bit editions •Microsoft Office LTSC for Mac 2021 •Microsoft 365 Apps for Enterprise for 64-bit Systems •Microsoft 365 Apps for Enterprise for 32-bit Systems •Microsoft Office Online Server •Microsoft Office 2019 for Mac •Microsoft Office 2019 for 64-bit editions •Microsoft Office 2019 for 32-bit editions •Microsoft SharePoint Server 2019 •Microsoft SharePoint Server 2019 •Microsoft SharePoint Enterprise Server 2013 Service Pack 1 •Microsoft SharePoint Enterprise Server 2013 Service Pack 1 •Microsoft SharePoint Enterprise Server 2016 •Microsoft SharePoint Enterprise Server 2016			
9	CIVN-2022-0009	Remote Code Execution vulnerabilities in Windows DirectX Graphics Kernel •Windows 10 Version 1909 for ARM64-based Systems •Windows 10 Version 1909 for x64-based Systems •Windows 10 Version 1909 for 32-bit Systems •Windows 10 Version 21H1 for 32-bit Systems •Windows 10 Version 21H1 for ARM64-based Systems •Windows 10 Version 21H1 for x64-based Systems •Windows 10 Version 21H2 for x64-based Systems •Windows 10 Version 21H2 for ARM64-based Systems •Windows 10 Version 21H2 for 32-bit Systems •Windows Server, version 20H2 (Server Core Installation)	Multiple vulnerabilities have been reported in Microsoft Windows DirectX Graphics Kernel which could be exploited by an attacker to execute arbitrary code on a targeted system.	HIGH	Apply appropriate updates as mentioned by the vendor https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21898 https://msrc.microsoft.com/update-

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows 10 Version 20H2 for ARM64-based Systems •Windows 10 Version 20H2 for 32-bit Systems •Windows 10 Version 20H2 for x64-based Systems •Windows Server 2022 (Server Core installation) •Windows Server 2022 •Windows Server 2019 (Server Core installation) •Windows Server 2019 •Windows 10 Version 1809 for ARM64-based Systems •Windows 10 Version 1809 for x64-based Systems •Windows 10 Version 1809 for 32-bit Systems			guide/vulnerability/CVE-2022-21912
12	CIVN-2022-0012	Multiple Vulnerabilities in Microsoft Edge (Chromium) •Microsoft Edge (Chromium) versions prior to 97.0.1072.55	Multiple vulnerabilities have been reported in Microsoft Edge (Chromium) which could allow a remote attacker to gain escalation of privileges and execute arbitrary code on the targeted system.	HIGH	Upgrade to Microsoft Edge version 97.0.1072.55 https://docs.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#january-6-2022
18	CIVN-2022-0018	Remote Code Execution Vulnerability in Microsoft's HTTP Protocol Stack •Windows Server, version 20H2 (Server Core Installation) •Windows Server 2022 (Server Core installation) •Windows Server 2022 •Windows Server 2019 (Server Core installation) •Windows Server 2019 •Windows 11 for x64-based Systems •Windows 11 for ARM64-based Systems	A vulnerability has been reported in Microsoft's HTTP Protocol Stack which could be exploited by an attacker to execute arbitrary code on the targeted system.	HIGH	Apply appropriate updates as mentioned by the vendor https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21907

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows 10 Version 21H2 for x64-based Systems •Windows 10 Version 21H2 for ARM64-based Systems •Windows 10 Version 21H2 for 32-bit Systems •Windows 10 Version 21H1 for x64-based Systems •Windows 10 Version 21H1 for ARM64-based Systems •Windows 10 Version 21H1 for 32-bit Systems •Windows 10 Version 20H2 for x64-based Systems •Windows 10 Version 20H2 for ARM64-based Systems •Windows 10 Version 20H2 for 32-bit Systems •Windows 10 Version 1809 for x64-based Systems •Windows 10 Version 1809 for ARM64-based Systems •Windows 10 Version 1809 for 32-bit Systems			
19	CIAD-2022-0001	Microsoft Windows	Security Feature Bypass, Elevation of Privilege, Denial of Service, Remote Code Execution, Information Disclosure, Spoofing	HIGH	Apply appropriate updates to windows as provided by Microsoft.