Vulnerability in various Products for August 01-31, 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 act ion taken in your organisation.

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
3	CIVN-2022-0316	Multiple Vulnerabilities in Google Chrome •Google Chrome versions prior to 104.0.5112.79	Multiple vulnerabilities have been reported in Google Chrome which could be exploited by an attacker to execute arbitrary code on the targeted system.	HIGH	Update to Google Chrome version 104.0.5112.79 as mentioned: https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html
4	CIVN-2022-0317	Multiple Vulnerabilities in Microsoft Edge (Chromium-based) •Microsoft Edge version prior to 104.0.1293.47	Multiple vulnerabilities have been reported in Microsoft Edge which could allow an attacker to execute arbitrary code, bypass security restrictions, and enable privilege escalation on the targeted system.	HIGH	Upgrade to Microsoft Edge version to 104.0.1293.47. https://msrc.microsoft.com/update-guide
7	CIVN-2022-0320	Remote Code Execution Vulnerabilities in Adobe Acrobat and Acrobat Reader •Acrobat DC and Acrobat Reader DC (Continuous) versions 22.002.20169 and earlier for Windows & MacOS. •Acrobat 2020 and Acrobat Reader 2020 (Classic 2020) versions 20.005.30362 and earlier for Windows & MacOS. •Acrobat 2017 and Acrobat Reader 2017 (Classic	Multiple vulnerabilities have been reported in Adobe Acrobat and Reader which could allow an attacker to execute arbitrary code on the target system.	HIGH	Apply appropriate updates as mentioned in the Adobe Security Bulletin: https://helpx.adobe.com/security/products/acrobat/apsb22-39.html

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		2017) versions 17.012.30249 and earlier for Windows & MacOS.			
8	CIVN-2022-0321	Remote Code Execution Vulnerability in Microsoft Windows Support Diagnostic Tool (MSDT) •Microsoft Windows 7 for 32-bit & x64 based Systems SP1 •Microsoft Windows RT version 8.1 •Microsoft Windows 8.1 for 32-bit & x64 systems •Microsoft Windows 10 for 32-bit & x64-based Systems •Microsoft Windows 10 Version 1607 for 32-bit & x64-based Systems •Microsoft Windows 10 Version 1809 for 32-bit, x64-based & ARM64-based Systems •Microsoft Windows 10 Version 20H2 for 32-bit, x64-based & ARM64-based Systems •Microsoft Windows 10 Version 21H1 for 32-bit, x64-based & ARM64-based Systems •Microsoft Windows 10 Version 21H2 for 32-bit, x64-based & ARM64-based Systems •Microsoft Windows 11 for 32-bit & x64-based Systems •Microsoft Windows Server 2008 R2 for x64-based Systems SP1 & x64-based Systems SP1 (Server Core installation) •Microsoft Windows Server version 20H2 (Server Core Installation) •Microsoft Windows Server 2012 & 2012 (Server Core installation) •Microsoft Windows Server 2012 R2 & 2012 R2 (Server Core installation) •Microsoft Windows Server 2016 & 2016 (Server	This vulnerability has been reported in Microsoft Windows Support Diagnostic Tool (MSDT) which could allow a remote attacker to execute arbitrary code on the target system.	HIGH	Apply appropriate updates as mentioned by vendor: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34713

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		Core installation) •Microsoft Windows Server 2019 & 2019 (Server Core installation) •Microsoft Windows Server 2022 & 2022 (Server Core installation)			
16	CIVN-2022-0329	Multiple Vulnerabilities in Google Chrome for Desktop •Google Chrome versions prior to 104.0.5112.101	Multiple vulnerabilities have been reported in Google Chrome which could allow an remote attacker to execute arbitrary code and Security restriction bypass on the targeted system.	HIGH	Update to Google Chrome version 104.0.5112.101 as mentioned: https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html
21	CIVN-2022-0334	Privilege escalation and security bypass vulnerabilities in Windows Defender Credential Guard •Windows 11 for ARM64-based Systems •Windows 11 for x64-based 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 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 20H2 for ARM64-based Systems •Windows 10 Version 20H2 for 32-bit Systems •Windows 10 Version 20H2 for x64-based Systems •Windows 10 Version 21H1 for 32-bit Systems	Privilege escalation and security bypass vulnerabilities have been reported in Windows Defender Credential Guard which could allow a local authenticated attacker to bypass security restrictions and gain elevated privileges on the targeted system.	HIGH	Apply appropriate patches as mentioned in Microsoft Security Bulletin. https://portal.msrc.microsoft.com/en-us/security-guidance

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows 10 Version 21H1 for ARM64-based Systems •Windows 10 Version 21H1 for x64-based Systems •Windows 10 Version 1809 for ARM64-based Systems •Windows 10 Version 1809 for x64-based Systems •Windows 10 Version 1809 for 32-bit Systems •Windows Server 2022 (Server Core installation) •Windows Server 2022 •Windows Server 2019 (Server Core installation) •Windows Server 2019 •Windows Server 2016 (Server Core installation) •Windows Server 2016 •Windows Server, version 20H2 (Server Core Installation)			
25	CIVN-2022-0338	Multiple Vulnerabilities in Mozilla Products •Mozilla Firefox Thunderbird versions prior to 91.13 & 102.2 •Mozilla Firefox ESR versions prior to 91.13 & 102.2 •Mozilla Firefox versions prior to 104	Multiple vulnerabilities have been reported in Mozilla products which could allow a remote attacker to bypass security restrictions, execute arbitrary code and cause denial of service attack on the targeted system.	HIGH	Upgrade to Mozilla Firefox Thunderbird versions 91.13 and 102.2, Firefox ESR versions 91.13 and 102.2, and Mozilla Firefox version 104