Vulnerability in various Products for February 11-20, 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
3	CIVN-2022-0087	Spoofing Vulnerability in Microsoft Edge (Chromium-based) •Microsoft Edge (Chromium-based) versions prior to 98.0.1108.50	A vulnerability has been reported in Microsoft Edge (Chromium-based) which could allow a remote attacker to perform spoofing attack on the targeted system.	HIGH	Upgrade to Microsoft Edge (Chromium-based) version 98.0.1108.50 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23264
9	CIVN-2022-0093	Multiple Vulnerabilities in Google Chrome •Google Chrome versions prior to 98.0.4758.102	Multiple vulnerabilities have been reported in Google Chrome which could allow a remote attacker to execute arbitrary code, bypass security restrictions or cause denial of service condition on the targeted system.	HIGH	Apply appropriate security updates as mentioned in below link: https://chromereleases.google-blog.com/2022/02/stable-channel-update-for-desktop_14.html
10	CIVN-2022-0094	Remote code execution vulnerability in Windows DNS server •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	A vulnerability has been reported in Windows DNS server which could be exploited by an attacker to execute arbitrary code on the targeted system.	MEDIUM	Apply appropriate updates as mentioned in: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21984

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows 10 Version 20H2 for x64-based 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 1909 for ARM64-based Systems •Windows 10 Version 1909 for x64-based Systems •Windows 10 Version 1909 for 32-bit Systems •Windows 11 for ARM64-based Systems •Windows 11 for x64-based Systems •Windows Server, version 20H2 (Server Core Installation) •Windows Server 2022 Azure Edition Core Hotpatch •Windows Server 2022 (Server Core installation) •Windows Server 2022			
12	CIVN-2022-0096	Multiple Vulnerabilities in Microsoft Edge (Chromium) •Microsoft Edge (Chromium) versions prior to 98.0.1108.55	Multiple vulnerabilities have been reported in Microsoft Edge (Chromium) which could allow a remote attacker to execute arbitrary code, bypass security restrictions or cause denial of service condition on the targeted system.	HIGH	Upgrade to Microsoft Edge version 98.0.1108.55 https://docs.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#february-16-2022
17	CIVN-2022-0101	Multiple vulnerabilities in Google Chrome OS •Google Chrome versions prior to 96.0.4664.194.	Multiple vulnerabilities have been reported in Google Chrome OS which could be exploited by a remote attacker to execute arbitrary code on the targeted system.	HIGH	Update to Google Chrome OS version 96.0.4664.194. https://chromereleases.googleblog.com/2022/02/long-term-support-channel-update_16.html