

Vulnerability in various Products for February 21-28, 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  <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23264">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23264</a>
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:  <a href="https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html">https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html</a>
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	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:  <a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21984">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21984</a>

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		<ul style="list-style-type: none"> <li>•Windows 10 Version 20H2 for 32-bit Systems</li> <li>•Windows 10 Version 20H2 for x64-based Systems</li> <li>•Windows 10 Version 21H1 for 32-bit Systems</li> <li>•Windows 10 Version 21H1 for ARM64-based Systems</li> <li>•Windows 10 Version 21H1 for x64-based Systems</li> <li>•Windows 10 Version 1909 for ARM64-based Systems</li> <li>•Windows 10 Version 1909 for x64-based Systems</li> <li>•Windows 10 Version 1909 for 32-bit Systems</li> <li>•Windows 11 for ARM64-based Systems</li> <li>•Windows 11 for x64-based Systems</li> <li>•Windows Server, version 20H2 (Server Core Installation)</li> <li>•Windows Server 2022 Azure Edition Core Hotpatch</li> <li>•Windows Server 2022 (Server Core installation)</li> <li>•Windows Server 2022</li> </ul>			
12	CIVN-2022-0096	<p>Multiple Vulnerabilities in Microsoft Edge (Chromium)</p> <ul style="list-style-type: none"> <li>•Microsoft Edge (Chromium) versions prior to 98.0.1108.55</li> </ul>	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	<p>Upgrade to Microsoft Edge version 98.0.1108.55</p> <p><a href="https://docs.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#february-16-2022">https://docs.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#february-16-2022</a></p>

<b>S No</b>	<b>CERT-in Vulnerability Note No</b>	<b>Product</b>	<b>Vulnerability Threat Description</b>	<b>Vulnerability Rating</b>	<b>Vendor URL/ Action</b>
17	CIVN-2022-0101	Multiple vulnerabilities in Google Chrome OS <ul style="list-style-type: none"> <li>•Google Chrome versions prior to 96.0.4664.194.</li> </ul>	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.  <a href="https://chromereleases.googleblog.com/2022/02/long-term-support-channel-update_16.html">https://chromereleases.googleblog.com/2022/02/long-term-support-channel-update_16.html</a>