Vulnerability in various Products for May 21-31, 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 action taken in your organisation.

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
13	CIVN-2022-0242	Multiple Vulnerabilities in Mozilla Products •Mozilla Firefox versions prior to 100.0.2 •Mozilla Firefox ESR versions prior to 91.9.1 •Mozilla Firefox for Android 100.3 •Mozilla Firefox Thunderbird versions prior to 91.9.1	Multiple vulnerabilities have been reported in Mozilla products which could allow a remote attacker to bypass security restrictions and execute arbitrary code on the targeted system.	HIGH	Upgrade to Mozilla Firefox version 100.0.2, Firefox ESR version 91.9.1, Firefox for Android 100.3 and Firefox Thunderbird versions prior to 91.9.1
17	CIVN-2022-0246	Multiple Vulnerabilities in Google Chrome •Google Chrome versions prior to 102.0.5005.61	Multiple vulnerabilities have been reported in Google Chrome which could allow a remote attacker to cause denial of service, bypass implemented security restrictions, gain access to sensitive information, and execute arbitrary code on the targeted systems.	HIGH	Update to Google Chrome version 102.0.5005.61 as mentioned: https://chromereleases.google-blog.com/2022/05/stable-channel-update-for-desktop_24.html

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
24	CIVN-2022-0253	Remote Code Execution Vulnerability in Microsoft Windows Support Diagnostic Tool (MSDT) •Windows 7 for 32-bit and x64-based Systems Service Pack 1 •Windows RT 8.1 •Windows 8.1 for 32-bit and x64-based systems •Windows 10 Version 1607 for 32-bit and x64-based Systems •Windows 10 for 32-bit and x64-based systems •Windows 10 Version 21H2 for 32-bit and x64-based systems •Windows 10 Version 21H2 for ARM64-based Systems •Windows 10 Version 20H2 for ARM64-based Systems •Windows 10 Version 20H2 for 32-bit and x64-based Systems •Windows 10 Version 21H1 for ARM64-based Systems •Windows 10 Version 21H1 for 32-bit and x64-based Systems •Windows 10 Version 1809 for 32-bit and x64-based systems •Windows 10 Version 1809 for ARM64-based Systems •Windows 11 for x64 and ARM64-based Systems •Windows Server, version 20H2 (Server Core Installation) •Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) •Windows Server 2008 R2 for x64-based Systems Service Pack 1 •Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) •Windows Server 2008 for x64-based Systems Service Pack 2	A vulnerability has been reported in Microsoft Windows Support Diagnostic Tool (MSDT) which could allow an attacker to execute arbitrary code on the targeted system.	HIGH	https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) •Windows Server 2008 for 32-bit Systems Service Pack 2 •Windows Server 2012 R2 (Server Core installation) •Windows Server 2012 R2 •Windows Server 2012 (Server Core installation) •Windows Server 2012 •Windows Server 2016 (Server Core installation) •Windows Server 2016 •Windows Server 2019 (Server Core installation) •Windows Server 2019 •Windows Server 2022 Azure Edition Core Hotpatch •Windows Server 2022 (Server Core installation) •Windows Server 2022			