Vulnerability in various Products for February 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
8	CIVN-2022-0067	Multiple Vulnerabilities in Google Chrome •Google Chrome versions prior to 98.0.4758.80	Multiple vulnerabilities have been reported in Google chrome which could allow an attacker to execute arbitrary code on the targeted system.	HIGH	Apply appropriate updates as mentioned https://chromereleases.google-blog.com/2022/02/stable-channel-update-for-desktop.html
11	CIVN-2022-0070	Multiple Vulnerabilities in Microsoft Edge (Chromium-based) •Microsoft Edge (Chromium-based) versions prior to 98.0.1108.43	Multiple vulnerabilities have been reported in Microsoft Edge (Chromium-based) which could allow a remote attacker to bypass of security restrictions, execute arbitrary code and gain escalated privileges on the targeted system.	HIGH	Upgrade to Microsoft Edge (Chromium-based) version 98.0.1108.43 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23261 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23262 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23263
12	CIVN-2022-0071	Multiple Vulnerabilities in Google Chrome OS •Google Chrome OS versions prior to 96.0.4664.180	Multiple vulnerabilities have been reported in Google Chrome OS which could be exploited by a remote attacker to bypass security restrictions, execute arbitrary code or cause denial	HIGH	Apply appropriate updates as mentioned https://chromereleases.google-blog.com/2022/02/long-term-support-channel-update.html

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
			of service condition on the targeted system.		
18	CIVN-2022-0077	Elevation of Privilege Vulnerability in Microsoft Windows Kernel •Windows Server 2012 R2 (Server Core installation) •Windows Server 2012 R2 •Windows Server 2012 (Server Core installation) •Windows Server 2012 •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 •Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) •Windows Server 2008 for 32-bit Systems	A vulnerability has been reported in Microsoft Windows Kernel which could allow an attacker to gain elevated privileges on the targeted system.	HIGH	Apply appropriate patches as mentioned by the vendor https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21989

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		Service Pack 2 •Windows RT 8.1 •Windows 8.1 for x64-based systems •Windows 8.1 for 32-bit systems •Windows 7 for x64-based Systems Service Pack 1 •Windows 7 for 32-bit Systems Service Pack 1 •Windows Server 2016 (Server Core installation) •Windows Server 2016 •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-			

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		based Systems •Windows 10 Version 21H2 for 32-bit Systems •Windows 11 for ARM64-based Systems •Windows 11 for x64-based Systems •Windows Server, version 20H2 (Server Core Installation) •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 Azure Edition Core Hotpatch •Windows Server 2022 (Server Core installation) •Windows Server 2022 •Windows 10 Version 21H1 for 32-bit Systems •Windows 10 Version 21H1 for ARM64-			

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		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 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			
22	CIVN-2022-0081	Multiple Vulnerabilities in Mozilla Products	Mozilla Firefox versions prior to 97Mozilla Firefox ESR versions prior to 91.6 Mozilla Firefox Thunderbird versions prior to 91.6	High	Upgrade to Mozilla Firefox version Firefox 97, Firefox ESR 91.6 and Firefox Thunderbird 91.6

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
23	CIVN-2022-0082	Multiple Vulnerabilities in Google Chrome OS •Google Chrome versions prior to 98.0.4758.91	Multiple vulnerabilities have been reported in Google Chrome OS which could be exploited by an attacker to execute arbitrary code on the targeted system.	HIGH	Update to Google Chrome OS version 98.0.4758.91 https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-chrome-os.html
25	CIVN-2022-0084	Elevation of Privilege Vulnerability in Windows Print Spooler •Windows Server 2012 R2 (Server Core installation) •Windows Server 2012 R2 •Windows Server 2012 (Server Core installation) •Windows Server 2012 •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 •Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) •Windows Server 2008 for 32-bit Systems Service Pack 2 •Windows RT 8.1 •Windows 8.1 for x64-based systems •Windows 8.1 for 32-bit systems	Multiple vulnerabilities have been reported in Windows Print Spooler which could allow an attacker to gain elevated privileges on the targeted system.	HIGH	Apply appropriate upgrade as mention: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22718 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22717 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21997 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21999

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows 7 for x64-based Systems Service Pack 1 •Windows 7 for 32-bit Systems Service Pack 1 •Windows Server 2016 (Server Core installation) •Windows Server 2016 •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 11 for ARM64-based Systems •Windows 11 for x64-based Systems •Windows Server, version 20H2 (Server Core Installation •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 Azure Edition Core Hotpatch			

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows Server 2022 (Server Core installation) •Windows Server 2022 •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 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			
26	CIAD-2022-0006	Microsoft Windows	Elevation of Privilege, Denial of Service, Remote Code Execution, Information Disclosure	HIGH	Apply appropriate updates to windows as provided by Microsoft as mentioned in URL below: https://msrc.microsoft.com/update-guide/releaseNote/2022-Feb