Vulnerability in various Products for September 11-20, 2021, 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-2021-XXXX, substituting XXXX with the number in second column

Kindly confirm action taken by your organisation/ Department.

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
4	CIVN-2021-0222	Microsoft Edge (Chromium-based) versions prior to 93.0.961.44	A vulnerability has been reported in Microsoft Edge (Chromium-based) which could allow a remote attacker to read-write access via tampering on a targeted system.	High	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38669
5	CIVN-2021-0223	Google Chrome Version prior to 93.0.4577.82	Multiple vulnerabilities have been reported in Google Chrome which could be exploited by an attacker to trigger remote code execution, denial of service condition and security restriction bypass on the targeted system.	High	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html
10	CIVN-2021-0228	•Mozilla Firefox for Android versions prior to92 •Mozilla Firefox ESR versions prior to 78.14 •Mozilla Firefox ESR versions prior to 91.1 •Mozilla Thunderbird for Windows versions prior to 78.14 •Mozilla Thunderbird for Windows versions prior to 91.1	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 Firefox for Android version 92, Firefox ESR 78.14, Firefox ESR 91.1, Thunderbird for Windows versions 78.14 and Thunderbird 91.1

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
12	CIVN-2021-0230	•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 Server, version 20H2 (Server Core Installation) •Windows 10 Version 20H2 for ARM64-based Systems •Windows 10 Version 20H2 for 32-bit and x64-based Systems •Windows Server, version 2004 (Server Core installation) •Windows 10 Version 2004 for 32-bit and x64-based Systems •Windows 10 Version 2004 for ARM64-based Systems •Windows 10 Version 21H1 for 32-bit and x64-based Systems •Windows 10 Version 21H1 for ARM64-based Systems •Windows 10 Version 1909 for ARM64-based Systems •Windows 10 Version 1909 for 32-bit and x64-based Systems •Windows 10 Version 1809 for ARM64-based Systems •Windows 10 Version 1809 for 32-bit and x64-based Systems	A vulnerability has been reported in Microsoft Windows Scripting Engine which could allow remote attacker to trigger memory corruption and execute arbitrary code on the targeted system.	High	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26435

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•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 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 (Server Core installation) •Windows Server 2022			
18	CIAD-2021-0033	•Windows •Microsoft Office •Developer Tools •Azure •Browser •Microsoft Dynamics	Multiple vulnerabilities have been reported in various Microsoft products, which could be exploited by an attacker to access sensitive information, bypass security restrictions, perform a denial of service (DoS) attack, escalating privileges, perform Spoofing attacks or executing arbitrary code on the targeted system.	High	https://msrc.microsoft.com/update-guide/releaseNote/2021-Sep