Vulnerability in various Products for December 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

Please update the below mentioned Software applications 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
4	CIVN-2021-0350	Multiple Vulnerabilities in Microsoft Edge (Chromium) •Microsoft Edge (Chromium) versions prior to 96.0.1054.53	Multiple vulnerabilities have been reported in Microsoft Edge (Chromium) which could allow a remote attacker to execute arbitrary code and bypass of security restrictions on the targeted system.	High	Upgrade to Microsoft Edge version 96.0.1054.53 https://docs.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#december-10-2021
5	CIVN-2021-0351	Multiple Vulnerabilities in Google Chrome •Google Chrome version prior to 96.0.4664.110	Multiple vulnerabilities have been reported in Google Chrome which could be exploited by a remote attacker to execute arbitrary code on the targeted system.	High	Apply appropriate security updates as mentioned in below link: https://chromereleases.googleblog.com/2021/12/stable-channel-update-for-desktop_13.html
7	CIVN-2021-0353	Multiple Vulnerabilities in Mozilla Products •Mozilla Firefox versions prior to 95	Multiple vulnerabilities have been reported in Mozilla products which could	High	Upgrade to Mozilla Firefox version Firefox 95, Firefox ESR 91.4.0 and

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Mozilla Firefox ESR versions prior to 91.4.0 •Mozilla Firefox Thunderbird versions prior to 91.4.0	allow a remote attacker to bypass security restriction, execute arbitrary code and cause denial of service attack on the targeted system.		Thunderbird 91.4.0
8	CIVN-2021-0354	Microsoft Windows Remote Desktop Client Remote Code Execution Vulnerability •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 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-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	A Remote Code Execution vulnerability has been reported in Microsoft Windows Remote Desktop Client which could be exploited by an attacker to execute arbitrary code on the targeted system.	High	Apply appropriate fix as mentioned in Microsoft Security Advisory https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43233

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows 10 Version 20H2 for 32-bit Systems •Windows 10 Version 20H2 for x64-based Systems •Windows Server, version 2004 (Server Core installation) •Windows 10 Version 2004 for x64-based Systems •Windows 10 Version 2004 for ARM64-based Systems •Windows 10 Version 2004 for 32-bit Systems •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			
18	CIAD-2021-0047	Multiple vulnerabilities in Microsoft product •Windows •Microsoft Office •Azure •Browser •Developer Tools •.NET	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 codes on the targeted system.	High	https://msrc.microsoft.com/update-guide/releaseNote/2021-Dec