

Vulnerability in various Products for April 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 in the enclosed compliance sheet.

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
1	CIVN-2021-0078	Google Chrome Version prior to 89.0.4389.114	Multiple vulnerabilities have been reported in Google chrome which could be exploited by an attacker to execute arbitrary code on the targeted system.	High	https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_30.html
3	CIVN-2021-0080	<ul style="list-style-type: none">•Microsoft Windows 10 Version 1803 for 32-bit Systems•Microsoft Windows 10 Version 1803 for x64-based Systems•Microsoft Windows 10 Version 1809 for 32-bit Systems•Microsoft Windows 10 Version 1809 for ARM64-based Systems•Microsoft Windows 10 Version 1809 for x64-based Systems•Microsoft Windows 10 Version 1909 for 32-bit Systems•Microsoft Windows 10 Version 1909 for ARM64-based Systems•Microsoft Windows 10 Version 1909	A vulnerability has been reported in Microsoft Windows which could allow a local attacker to obtain elevated privileges on the targeted system.	High	https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2021-28310

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		<ul style="list-style-type: none"> for x64-based Systems •Microsoft Windows 10 Version 2004 for 32-bit Systems •Microsoft Windows 10 Version 2004 for ARM64-based Systems •Microsoft Windows 10 Version 2004 for x64-based Systems •Microsoft Windows 10 Version 20H2 for 32-bit Systems •Microsoft Windows 10 Version 20H2 for ARM64-based Systems •Microsoft Windows 10 Version 20H2 for x64-based Systems •Microsoft Windows Server 2019 •Microsoft Windows Server 2019 (Server Core installation) •Microsoft Windows Server, version 1909 (Server Core installation) •Microsoft Windows Server, version 2004 (Server Core installation) •Microsoft Windows Server, version 20H2 (Server Core Installation) 			
4	CIVN-2021-0081	Google Chrome versions prior to 89.0.4389.128	Multiple vulnerabilities have been reported in Google Chrome which could be exploited by an attacker to execute arbitrary code on a targeted system.	High	https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop.html
7	CIAD-2021-0015	<ul style="list-style-type: none"> •Windows •Microsoft Office 	Multiple vulnerabilities have been reported in	High	https://msrc.microsoft.com/update-guide/en-us/releaseNote/2021-Apr

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		<ul style="list-style-type: none"> •Extended Security Updates (ESU) •Developer Tools •Azure •Exchange Server 	<p>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.</p>		