Vulnerability in various Products for May 01 -10, 2020, 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-2020-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**
14	CIVN-2020-0126	Google Chrome versions prior to 81.0.4044.129	Multiple vulnerabilities have been reported in Google Chrome which could enable a remote attacker to take control of an exploited system.	HIGH	Upgrade to latest Google Chrome version 81.0.4044.129 or later: https://support.google.com/chrome/answer/95414
16	CIVN-2020-0132	Mozilla Firefox for iOS versions: 8.0, 9.0, 10.0, 11.0, 12.0, 13.0, 14.0, 15.0, 16.0, 17.0, 18.0, 19.0, 20.0, 21.0, 22.0, 23.0, 24.0	It could allow a remote attacker to obtain sensitive information.	LOW	https://www.mozilla.org/en-US/security/advisories/mfsa2020-15/
19	CIVN-2020-0136	Google Android versions 8.0, 8.1, 9, 10	It could allow a remote attacker to gain elevated privileges, obtain sensitive information, execute remote code and cause	HIGH	Apply over-the-air updates https://source.android.com/security/bulletin/2020-05-01

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
			Denial of service condition on the targeted system.		
20	CIAD-2020-0027	Securing Microsoft Office 365 services	Best Practices for Office 365	HIGH	https://docs.microsoft.com/en-us/microsoft-365/security/mtp/overview-security-center
28	CIVN-2020-0142	Mozilla Firefox versions prior to 76.0 Mozilla Firefox ESR versions prior to 68.8 Mozilla Firefox Thunderbird versions prior to 68.8	It could allow a remote attacker to bypass security restrictions, obtain sensitive information, execute arbitrary code on the target system, spoof the address bar or cause denial of service (DoS) conditions.	HIGH	https://www.mozilla.org/en-US/security/advisories/mfsa2020-18/ https://www.mozilla.org/en-US/security/advisories/mfsa2020-17/ https://www.mozilla.org/en-US/security/advisories/mfsa2020-16/
29	CIVN-2020-0140	Google Chrome versions prior to 81.0.4044.138-1	It could allow a remote attacker to execute arbitrary code on the targeted system.	HIGH	Upgrade to Google Chrome version 81.0.4044.138-1 https://chromereleases.googleblog.com/2020/05/stable-channel-update-for-desktop.html