Vulnerability in various Products for June 21-30, 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
3	CIVN-2021-0149	•Google Chrome versions prior to 91.0.4472.114	Multiple vulnerabilities have been reported in Google Chrome which could be exploited by a remote attacker to compromise a targeted system.	High	Upgrade to Google Chrome 91.0.4472.114 https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop_17.html
10	CIVN-2021-0156	•Dell Alienware m15 R6 •Dell G15, G3, G5, G7 •Dell Inspiron •Dell OptiPlex •Dell Latitude •Dell Precision •Dell Vostro •Dell XPS	Multiple vulnerabilities have been reported in the BIOSConnect and HTTPS Boot features of Dell Client BIOS which could allow an attacker to execute arbitrary code or cause denial of service conditions.	High	https://www.dell.com/support/kbdoc/en-in/000188682/dsa-2021-106-dell-client-platform-security-update-for-multiple-vulnerabilities-in-the-supportassist-biosconnect-feature-and-https-boot-feature
14	CIAD-2021-0022	•Windows 10 for 32-bit Systems and x64-based Systems •Windows 10 Version 1607 for 32-bit Systems and x64-based Systems •Windows 10 Version 1809 for 32-bit Systems, x64-based Systems and ARM64-based Systems	A vulnerability in Print Spooler service of Microsoft Windows, being termed as "PrintNightmare", has been reported which could be exploited by a remote attacker to execute arbitrary code on a targeted system.	High	Microsoft is currently assessing the vulnerability and no patches are available yet. Users are advised to check the following webpage for updates: https://msrc.microsoft.com/update-

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows 10 Version 1909 for 32-bit Systems, x64-based Systems and ARM64-based Systems •Windows 10 Version 2004 for 32-bit Systems, x64-based Systems and ARM64-based Systems •Windows 10 Version 20H2 for 32-bit Systems, x64-based Systems and ARM64-based Systems •Windows 10 Version 21H1 for 32-bit Systems, x64-based Systems and ARM64-based Systems •Windows 7 for 32-bit Systems SP1 and x64-based Systems SP1 •Windows 8.1 for 32-bit systems and x64-based Systems SP1 •Windows RT 8.1 •Windows Server 2008 for 32-bit Systems SP2 •Windows Server 2008 for x64-based Systems SP2 •Windows Server 2008 R2 for x64-based Systems SP1 •Windows Server 2012 •Windows Server 2012 R2 •Windows Server 2016 •Windows Server 2019 •Windows Server 2008 for 32-bit Systems SP2 (Server Core installation) and x64-based Systems SP2 (Server Core installation)			guide/vulnerability/CVE-2021-34527

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows Server 2008 R2 for x64-based Systems SP1 (Server Core installation) •Windows Server 2012 (Server Core installation) •Windows Server 2012 R2 (Server Core installation) •Windows Server 2016 (Server Core installation) •Windows Server 2019 (Server Core installation) •Windows Server, version 2004 (Server Core installation) •Windows Server, version 20H2 (Server Core Installation)			