Vulnerability in various Products for October 21-31, 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.

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
1	CIVN-2021-0270	All Apache OpenOffice prior to versions 4.1.10	Multiple vulnerabilities have been reported in Apache OpenOffice which could be exploited by an attacker to bypass security restrictions, execute arbitrary code and can cause Denial of Service condition on the targeted system.	Medium	Upgrade to Apache OpenOffice version 4.1.11: https://www.openoffice.org/download/
2	CIVN-2021-0271	Google Chrome Version prior to 95.0.4638.54	Multiple vulnerabilities have been reported in Google chrome which could be exploited by a remote attacker to bypass security restrictions to gain access to sensitive information and execute arbitrary code on the targeted system.	High	Upgrade to Google chrome version 95.0.4638.54 https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html
19	CIVN-2021-0288	•Windows Server 2012 R2 (Server Core installation) •Windows Server 2012 R2 •Windows Server 2012 (Server Core installation) •Windows Server 2012	A vulnerability has been reported in Microsoft Windows user profile service which could allow a local attacker to gain elevated privileges on the targeted system.	High	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34484

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 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 Server, version 20H2 (Server Core Installation)			

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows 10 Version 20H2 for ARM64-based Systems •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 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			

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows 10 Version 1809 for x64-based Systems •Windows 10 Version 1809 for 32-bit Systems			
21	CIVN-2021-0290	Google chrome version prior to 95.0.4638.69	Multiple vulnerabilities have been reported in Google chrome which could be exploited by a remote attacker to bypass security restrictions to gain access to sensitive information and execute arbitrary code on the targeted system.	High	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.html
23	CIAD-2021-0041	•Windows •Microsoft Office •Developer Tools •System Center •Browser •Microsoft Dynamics •.NET 5.0 •Intune management extension	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/release-Note/2021-Oct