Vulnerability in various Products for April 11-20, 2022, 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-2022-XXXX, substituting XXXX with the number in second column

Please update the below mentioned applications/window's version 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
2	CIVN-2022-0175	Multiple Vulnerabilities in Google Chrome •Google Chrome Version prior to 100.0.4896.88	Multiple vulnerabilities have been reported in Google Chrome which could allow a remote attacker to execute arbitrary code and access sensitive information on the targeted system.	HIGH	Upgrade to Google chrome version 100.0.4896.88: https://chromereleases.googleblog.com/2022/04/stable-channel-update-for-desktop_11.html
4	CIVN-2022-0177	Remote Code Execution Vulnerability in Windows Remote Procedure Call Runtime •Windows 7 for 32-bit Systems Service Pack 1 •Windows Server 2016 (Server Core installation) •Windows 11 for ARM64-based Systems •Windows Server, version 20H2 (Server Core Installation) •Windows 10 Version 20H2 for ARM64-based Systems •Windows 10 Version 1909 for ARM64-based Systems •Windows 10 Version 1809 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 10 Version 1809 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	A vulnerability has been reported in Windows Remote Procedure Call Runtime which could allow a remote attacker to execute arbitrary code on the targeted system.	CRITICAL	Apply appropriate upgrade as mention: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26809

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows 10 Version 21H1 for x64-based Systems •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 10 Version 20H2 for 32-bit Systems •Windows 10 Version 20H2 for x64-based Systems •Windows Server 2008 for x64-based Systems Service Pack 2 (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 Version 1909 for x64-based Systems •Windows 10 Version 1909 for 32-bit Systems •Windows 10 Version 1809 for ARM64-based Systems •Windows Server 2008 for x64-based Systems Service Pack 2 •Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) •Windows 8.1 for 32-bit systems •Windows 7 for x64-based Systems Service Pack 1 •Windows Server 2008 for 32-bit Systems Service Pack 2 •Windows RT 8.1 •Windows 8.1 for x64-based systems •Windows 11 for x64-based Systems •Windows Server 2019 (Server Core installation) •Windows Server 2019			
6	CIVN-2022-0179	Elevation of Privilege Vulnerability in Windows User Profile Service •Windows Server 2012 R2 (Server Core installation)	A vulnerability has been reported in Windows User Profile Service which could allow an attacker to	HIGH	Apply appropriate upgrade as mention:

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows Server 2008 for 32-bit Systems Service Pack 2 •Windows RT 81 •Windows 81 for x64-based systems •Windows 81 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 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 •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 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 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 2022 (Server Core installation)	gain elevated privileges on the targeted system.		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26904

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•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 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			
7	CIVN-2022-0180	Remote Code Execution Vulnerability in Windows SMB •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 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	A vulnerability has been reported in Windows SMB which could allow a remote attacker to execute arbitrary code on the targeted system.	HIGH	Apply appropriate upgrade as mentioned below: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-24500

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•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 •Windows 10 Version 20H2 for 32-bit Systems •Windows 10 Version 20H2 for x64-based 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			
8	CIVN-2022-0181	Elevation of Privilege Vulnerability in Windows Common Log File System Driver •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	A vulnerability has been reported in Windows Common Log File System Driver which could allow an attacker to gain elevated privileges on the targeted system.	HIGH	Apply appropriate upgrade as mention: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-24521

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		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 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 •Windows 10 Version 20H2 for 32-bit Systems •Windows 10 Version 20H2 for x64-based 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			

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•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			
9	CIVN-2022-0182	Remote Code Execution Vulnerability in Windows Network File System •Windows Server 2012 R2 (Server Core installation) •Windows Server 2012 R2 •Windows Server 2012 (Server Core installation) •Windows Server 2012 •Windows RT 8.1 •Windows 8.1 for x64-based systems •Windows 8.1 for 32-bit systems •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 •Windows 10 Version 20H2 for 32-bit Systems •Windows 10 Version 20H2 for x64-based 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	A vulnerability has been reported in Windows Network File System which could allow a remote attacker to execute arbitrary code on the targeted system.	HIGH	Apply appropriate upgrade as mention: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-24491

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•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			
11	CIVN-2022-0184	Remote Code Execution Vulnerability in Microsoft Windows LDAP •Windows 7 for 32-bit Systems and x64-based Systems Service Pack 1 •Windows RT 8.1 •Windows 8.1 for 32-bit Systems and x64-based Systems •Windows 10 Version 1607 for 32-bit Systems and x64-based Systems •Windows 10 for 32-bit Systems and x64-based Systems •Windows 10 Version 21H2 for 32-bit Systems, x64-based Systems &ARM64-based Systems •Windows 10 Version 1809 for 32-bit Systems, x64-based Systems &ARM64-based Systems •Windows 10 Version 20H2 for 32-bit Systems, x64-based Systems &ARM64-based Systems •Windows 10 Version 21H1 for 32-bit Systems, x64-based Systems &ARM64-based Systems •Windows 10 Version 1909 for 32-bit Systems, x64-based Systems &ARM64-based Systems •Windows 11 for x64-based Systems & ARM64-based Systems •Windows Server, version 20H2 (Server Core Installation) •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	A vulnerability has been reported in Microsoft Windows LDAP which could allow a remote attacker to execute remote code on the targeted system.	HIGH	Apply appropriate patches as mentioned in Microsoft Security Bulletin https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26919

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		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 Server 2012 (Server Core installation) •Windows Server 2012 •Windows Server 2016 (Server Core installation) •Windows Server 2016 •Windows Server 2019 (Server Core installation) •Windows Server 2019 •Windows Server 2022 (Server Core installation) •Windows Server 2022			
15	CIVN-2022-0188	Multiple Vulnerabilities in Adobe Acrobat and Reader •Acrobat DC 22.001.20085 and earlier versions for Windows and macOS •Acrobat Reader DC 22.001.20085 and earlier versions for Windows and macOS •Acrobat 2020 20.005.30314 and earlier versions for Windows •Acrobat 2020 20.005.30311 and earlier versions for macOS •Acrobat Reader 2020 20.005.30314 and earlier versions for Windows •Acrobat Reader 2020 20.005.30311 and earlier versions for macOS •Acrobat 2017 17.012.30205 and earlier versions for Windows and macOS •Acrobat Reader 2017 17.012.30205 and earlier versions for Windows and macOS	Multiple vulnerabilities have been reported in Adobe Acrobat and Reader which could allow an attacker to execute arbitrary code, memory leak, security feature bypass and privilege escalation on the targeted system.	HIGH	Apply appropriate upgrade as mentioned below: https://helpx.adobe.com/security/products/acrobat/apsb22-16.html
18	CIVN-2022-0191	Remote Code Execution Vulnerability in Windows Server Service •Windows Server 2012 R2 (Server Core installation) •Windows Server 2012 R2	A vulnerability has been reported in Windows server service which could allow a remote attacker to	HIGH	Apply appropriate upgrade as mentioned below:

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•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 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 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 •Windows 10 Version 20H2 for 32-bit Systems •Windows 10 Version 20H2 for x64-based Systems •Windows Server 2022 (Server Core installation) •Windows Server 2022	gain elevated privileges on the targeted system.		https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-24541

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•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			
22	CIVN-2022-0195	Multiple Vulnerabilities in Microsoft Edge (Chromium-based) •Microsoft Edge version prior to 100.0.1185.44	Multiple vulnerabilities have been reported in Microsoft Edge (Chromium-based) which could be exploited by an attacker to compromise targeted system.	HIGH	Upgrade to Microsoft Edge version to 100.0.1185.44. https://msrc.microsoft.com/update-guide