Vulnerability in various Products for September 01-30, 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 act ion taken in your organisation.

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
4	CIVN-2022-0343	Multiple Vulnerabilities in Google Chrome for Desktop •Google Chrome versions prior to 105.0.5195.52	Multiple vulnerabilities have been reported in Google Chrome for desktop which could be exploited by an attacker to execute arbitrary code on the targeted system.	HIGH	Update to Google Chrome version 105.0.5195.52 as mentioned: https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html
5	CIVN-2022-0344	Security Bypass Vulnerability in Google Chrome •Google Chrome for Desktop versions prior to 105.0.5195.102 (for Windows, Mac and Linux)	A vulnerability has been reported in Google Chrome for desktop which could allow an attacker to bypass security restrictions on the targeted system.	HIGH	Update to Google Chrome version 105.0.5195.102 as mentioned by the vendor https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop.html
14	CIVN-2022-0353	Remote Code Execution Vulnerability in Windows TCP/IP •Windows Server 2022 Azure Edition Core Hotpatch •Windows Server 2022 (Server Core installation) •Windows Server 2022 •Windows Server 2019 (Server Core installation)	A vulnerability has been reported in Microsoft Windows TCP/IP which could allow an unauthenticated remote attacker to execute arbitrary code on the targeted system.	HIGH	Apply appropriate upgrade as mention: https://msrc.microsoft.com/update-

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		•Windows Server 2019 •Windows Server 2016 (Server Core installation) •Windows Server 2016 •Windows Server 2012 R2 (Server Core installation) •Windows Server 2012 R2 •Windows Server 2012 (Server Core installation) •Windows Server 2012 •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 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 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 11 for x64-based Systems •Windows 11 for ARM64-based 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 10 Version 21H1 for x64-based Systems •Windows 10 Version 21H1 for ARM64-based Systems			guide/en-US/vulnerability/CVE-2022-34718

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 20H2 for x64-based Systems •Windows 10 Version 20H2 for ARM64-based Systems •Windows 10 Version 20H2 for 32-bit Systems •Windows 10 Version 1809 for x64-based Systems •Windows 10 Version 1809 for ARM64-based Systems •Windows 10 Version 1809 for 32-bit Systems •Windows 10 Version 1607 for x64-based Systems •Windows 10 Version 1607 for 32-bit Systems			
15	CIVN-2022-0354	Elevation of Privilege Vulnerability in Windows Common Log File System Driver •Windows Server 2022 Azure Edition Core Hotpatch •Windows Server 2022 (Server Core installation) •Windows Server 2022 •Windows Server 2019 (Server Core installation) •Windows Server 2019 •Windows Server 2016 (Server Core installation) •Windows Server 2016 •Windows Server 2012 R2 (Server Core installation) •Windows Server 2012 R2 •Windows Server 2012 (Server Core installation) •Windows Server 2012 •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 Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	A vulnerability has been reported in Windows Common Log File System Driver which could allow a local user to escalate privileges on the targeted system.	HIGH	Apply appropriate upgrade as mention: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-37969

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 •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 11 for x64-based Systems •Windows 11 for ARM64-based 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 10 Version 21H1 for x64-based Systems •Windows 10 Version 21H1 for ARM64-based Systems •Windows 10 Version 21H1 for 32-bit Systems •Windows 10 Version 20H2 for x64-based Systems •Windows 10 Version 20H2 for ARM64-based Systems •Windows 10 Version 20H2 for 32-bit Systems •Windows 10 Version 1809 for x64-based Systems •Windows 10 Version 1809 for ARM64-based Systems •Windows 10 Version 1809 for 32-bit Systems •Windows 10 Version 1607 for x64-based Systems •Windows 10 Version 1607 for 32-bit Systems			
20	CIVN-2022-0359	Multiple Vulnerabilities in Google Chrome for Desktop •Google Chrome versions prior to 105.0.5195.125	Multiple Vulnerabilities have been reported in Google Chrome for Desktop which could be exploited by a remote attacker to bypass security restriction, execute arbitrary code or cause denial of service condition on the targeted system.	HIGH	Apply appropriate updates as mentioned: https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_14.html

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
25	CIVN-2022-0364	Multiple Vulnerabilities in Microsoft Edge •Microsoft Edge version prior to 105.0.1343.42	Multiple vulnerabilities have been reported in Microsoft Edge which could allow a remote attacker to execute arbitrary code or cause denial of service condition on the targeted system.	HIGH	Apply appropriate software updates as mentioned in the below link: https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#september-15-2022
28	CIVN-2022-0367	Multiple vulnerabilities in Mozilla Firefox •Mozilla Firefox versions prior to 105 •Mozilla Firefox ESR versions prior to 102.3	Multiple Vulnerabilities have been reported in Mozilla Firefox which could be exploited by a remote attacker to bypass security restriction, execute arbitrary code and disclose sensitive information on the targeted system.	HIGH	Upgrade to Mozilla Firefox version 105 and Mozilla Firefox ESR version 102.3
33	CIVN-2022-0372	Multiple Vulnerabilities in Google Chrome for Desktop •Google Chrome versions prior to 106.0.5249.61 for Mac/linux and 106.0.5249.61/62 for Windows	Multiple Vulnerabilities have been reported in Google Chrome for Desktop which could be exploited by a remote attacker to bypass security restriction, execute arbitrary code or cause denial of service condition on the targeted system.	HIGH	Apply appropriate updates as mentioned https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html