Vulnerability in various Products for November 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**
5	CIVN-2022-0418	Remote code execution vulnerability in Google Chrome •Google Chrome versions prior to 107.0.5304.87 for Mac and Linux •Google Chrome versions prior to 107.0.5304.87/.88 for Windows	A vulnerability has been reported in Google Chrome which could allow a remote attacker to execute arbitrary code on the targeted system.	HIGH	Apply appropriate updates as mentioned by vendor. https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_27.html
6	CIVN-2022-0419	Remote code execution vulnerability in Microsoft Edge •Microsoft Edge version prior to 107.0.1418.26	A vulnerability has been reported in Microsoft Edge which could allow a remote attacker to execute arbitrary code on the targeted system.	HIGH	Apply appropriate updates as mentioned by vendor. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3723

18	CIVN-2022-0431	Privilege Escalation Vulnerability in Microsoft Windows •Windows 7 for x64-based Systems Service Pack 1 •Windows 7 for x64-based Systems Service Pack 1 •Windows 7 for 32-bit 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 22H2 for 32-bit Systems •Windows 10 Version 22H2 for ARM64-based Systems •Windows 10 Version 22H2 for x64-based Systems •Windows 11 Version 22H2 for x64-based Systems •Windows 11 Version 22H2 for ARM64-based 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 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 Datacenter: Azure Edition (Hotpatch) •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 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	A vulnerability has been reported in Microsoft Windows, which could allow an attacker to perform privilege escalation on the targeted system.	CRITICAL	Apply appropriate fix/patches as mentioned in the following link https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41073

19	CIVN-2022-0432	Remote code execution vulnerability in Microsoft Windows •Windows Server 2022 Datacenter: Azure Edition (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 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 32-bit systems and x64-based systems •Windows 7 for 32-bit Systems and x64-based Systems Service Pack 1 •Windows 11 for x64-based Systems and ARM64-based Systems •Windows 11 Version 22H2 for x64-based Systems and ARM64-based Systems •Windows 10 for 32-bit Systems and x64-based Systems •Windows 10 Version 22H2 for 32-bit Systems, x64-based Systems and ARM64-based Systems •Windows 10 Version 21H2 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 10 Version 20H2 for 32-bit Systems, x64-based Systems and ARM64-based Systems •Windows 10 Version 1809 for 32-bit Systems ,x64-based Systems and ARM64-based Systems •Windows 10 Version 1607 for 32-bit Systems and x64-based Systems	These vulnerabilities have been reported in Microsoft Windows which could allow a remote attacker to execute arbitrary code on the targeted system.	HIGH	Apply appropriate patches as mentioned in Microsoft Security Bulletin: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41039 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41088 https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41128 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41118 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41044

22	CIVN-2022-0435	Privilege Escalation Vulnerability in Microsoft Windows •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 22H2 for 32-bit Systems •Windows 10 Version 22H2 for ARM64-based Systems •Windows 10 Version 22H2 for x64-based Systems •Windows 11 Version 22H2 for x64-based Systems •Windows 11 Version 22H2 for ARM64-based 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 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 Datacenter: Azure Edition (Hotpatch) •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 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	A vulnerability has been reported in Microsoft Windows which could allow an attacker to perform privilege escalation on the targeted system.	MEDIUM	Apply appropriate fix/patches as mentioned in the following link https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41125

29	CIVN-2022-0442	Security Features Bypass Vulnerability in Microsoft Windows •Windows 10 Version 22H2 for x64-based Systems, 32-bit Systems, ARM64-based Systems •Windows 11 Version 22H2 for x64-based Systems, ARM64-based Systems •Windows Server 2016 •Windows Server 2016 (Server Core installation) •Windows 10 Version 1607 for x64-based Systems, 32-bit Systems •Windows 10 for x64-based Systems, 32-bit Systems •Windows 10 Version 21H2 for x64-based Systems, 32-bit Systems, ARM64-based Systems •Windows 11 for ARM64-based Systems, x64-based Systems •Windows 10 Version 20H2 for ARM64-based Systems, 32-bit Systems, x64-based Systems •Windows Server 2022 Datacenter: Azure Edition (Hotpatch) •Windows Server 2022 (Server Core installation) •Windows Server 2022 •Windows 10 Version 21H1 for 32-bit Systems, ARM64-based Systems, x64-based Systems •Windows Server 2019 (Server Core installation) •Windows Server 2019 •Windows 10 Version 1809 for ARM64-based Systems, x64-based Systems, 32-bit Systems	A vulnerability has been reported in Microsoft Windows which could allow a remote attacker to bypass security restriction on the targeted system.	MEDIUM	Apply appropriate patches as mentioned by vendor https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41091
30	CIVN-2022-0443	Multiple Vulnerabilities in Microsoft Edge (Chromium-based) •Microsoft Edge (Chromium-based) version prior to 107.0.1418.42	Multiple vulnerabilities have been reported in Microsoft Edge (Chromium-based), which could be exploited by an attacker to execute arbitrary code on the targeted system.	HIGH	Upgrade to Microsoft Edge version 107.0.1418.42 https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#november-10-2022

41	CIVN-2022-0454	Multiple vulnerabilities in Mozilla Products •Mozilla Firefox versions prior to 107 •Mozilla Firefox ESR versions prior to 102.5 •Mozilla Thunderbird versions prior to 102.5	Multiple vulnerabilities have been reported in Mozilla products, which could allow an attacker to bypass security restrictions, execute arbitrary code, gain access to potentially sensitive information, perform Cross-Site Scripting (XSS) attacks, perform spoofing attacks or cause a denial of service (DoS) condition on the targeted system.	HIGH	Apply appropriate software updates as mentioned in the Mozilla Security Advisory: https://www.mozilla.org/en-US/security/advisories/mfsa2022-47/ https://www.mozilla.org/en-US/security/advisories/mfsa2022-48/ https://www.mozilla.org/en-US/security/advisories/mfsa2022-49/
48	CIVN-2022-0461	Remote code execution vulnerability in Google Chrome •Google Chrome versions prior to 107.0.5304.121 for Mac and Linux •Google Chrome versions prior to 107.0.5304.121/.122 for Windows	A Vulnerability has been reported in Google Chrome, which could allow a remote attacker to execute arbitrary code on the targeted system.	HIGH	Apply appropriate updates as mentioned by the vendor. https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop_24.html
49	CIVN-2022-0462	Remote code execution vulnerability in Microsoft Edge (Chromium-based) •Microsoft Edge (Chromium-based) version prior to 107.0.1418.62	A Vulnerability has been reported in Microsoft Edge (Chromium-based), which could allow a remote attacker to execute arbitrary code on the targeted system.	HIGH	Upgrade to Microsoft Edge version 107.0.1418.62 https://learn.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#november-28-2022

66	CIVN-2022-0479	Multiple Vulnerabilities in Mozilla Products •Mozilla Firefox versions prior to 108 •Mozilla Firefox ESR versions prior to 102.6 •Mozilla Thunderbird versions prior to 102.6	Multiple vulnerabilities have been reported in Mozilla Firefox, Mozilla Thunderbird and Mozilla Firefox ESR which could be exploited by a remote attacker to perform spoofing attack, execute arbitrary code, bypass security restrictions, gain access to potentially sensitive information, perform memory corruption and a potentially exploitable crash on the targeted system.	HIGH	Apply appropriate fixes as mentioned in Mozilla Security advisories: https://www.mozilla.org/en-US/security/advisories/mfsa2022-51 https://www.mozilla.org/en-US/security/advisories/mfsa2022-52 https://www.mozilla.org/en-US/security/advisories/mfsa2022-53