

Vulnerability in various Products for May 01-10, 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
1	CIVN-2022-0207	Multiple vulnerabilities in Google Chrome OS •Google Chrome OS versions prior to 96.0.4664.207.	Multiple vulnerabilities have been reported in Google Chrome OS which could be exploited by an attacker to execute arbitrary code on the targeted system.	HIGH	Update to Google Chrome OS version 96.0.4664.207. https://chromereleases.googleblog.com/2022/04/long-term-support-channel-update_28.html
3	CIVN-2022-0209	Multiple Vulnerabilities in Microsoft Edge (Chromium-based) •Microsoft Edge versions prior to 101.0.1210.32	Multiple vulnerabilities have been reported in Microsoft Edge server which could be exploited by an attacker to gain elevated privileges on the targeted system.	MEDIUM	Apply appropriate updates as mentioned in: https://msrc.microsoft.com/update-guide
8	CIVN-2022-0214	Multiple Vulnerabilities in Mozilla Products •Mozilla Firefox Thunderbird versions prior to 91.9 •Mozilla Firefox ESR versions prior to 91.9 •Mozilla Firefox versions prior to 100	Multiple vulnerabilities have been reported in Mozilla Products which could allow a remote attacker to execute arbitrary code and bypass security restrictions on the targeted system.	HIGH	Upgrade to Mozilla Firefox version 100, Firefox ESR version 91.9 and Firefox Thunderbird version 91.9
13	CIVN-2022-0219	Multiple vulnerabilities in Google Chrome for Android •Google Chrome versions prior to 101.0.4951.61	Multiple vulnerabilities have been reported in Google Chrome which could be exploited by an	HIGH	Update to Google Chrome version 101.0.4951.61 as mentioned

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
			attacker to execute arbitrary code on the targeted system.		https://chromereleases.googleblog.com/2022/05/chrome-for-android-update.html
16	CIVN-2022-0222	Privilege Escalation Vulnerability in Microsoft Active Directory Domain Services <ul style="list-style-type: none"> •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 and ARM64-based Systems •Windows 11 for 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 10 Version 1909 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 	A vulnerability has been reported in Microsoft Active Directory Domain Services which could allow a remote attacker to gain elevated privileges on the targeted system.	CRITICAL	Apply appropriate upgrade as mentioned: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26923
17	CIVN-2022-0223	Remote Code Execution Vulnerability in Microsoft Windows Fax Compose Form <ul style="list-style-type: none"> •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 for 32-bit Systems •Windows 10 Version 21H2 for 32-bit Systems, x64-based Systems and ARM64-based Systems •Windows 11 for x64-based Systems and ARM64-based Systems •Windows 10 Version 1607 for 32-bit Systems •Windows 10 for x64-based Systems 	A vulnerability has been reported in Microsoft Windows Fax Compose Form which could allow a remote attacker to execute arbitrary code on the targeted system.	CRITICAL	Apply appropriate upgrade as mentioned: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26917

S No	CERT-in Vulnerability Note No	Product	Vulnerability Threat Description	Vulnerability Rating	Vendor URL/ Action
		<ul style="list-style-type: none"> •Windows 8.1 for 32-bit systems •Windows 10 Version 1909 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 RT 8.1 •Windows 8.1 for x64-based systems •Windows 7 for x64-based Systems Service Pack 1 •Windows 7 for 32-bit Systems Service Pack 1 •Windows 10 Version 1607 for x64-based Systems 			
23	CIVN-2022-0229	<p>Multiple vulnerabilities in Google Chrome</p> <ul style="list-style-type: none"> •Google Chrome versions prior to 101.0.4951.64 	<p>Multiple vulnerabilities have been reported in Google Chrome which could be exploited by an attacker to execute arbitrary code on the targeted system.</p>	HIGH	<p>Update to Google Chrome version 101.0.4951.64 as mentioned:</p> <p>https://chromereleases.googleblog.com/2022/05/stable-channel-update-for-desktop_10.html</p>
24	CIAD-2022-0013	<p>Multiple vulnerabilities in Microsoft product</p> <ul style="list-style-type: none"> •Microsoft Windows 	<p>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, escalate privileges, perform Spoofing attacks or execute arbitrary codes on the targeted system.</p>	HIGH	<p>Apply appropriate security updates as mentioned in:</p> <p>https://msrc.microsoft.com/update-guide/releaseNote/2022-May</p>