Source : www.thehindu.com Date : 2022-08-14

CERT-IN DETECTS MULTIPLE VULNERABILITIES IN CHROME, EDGE BROWSERS AND ANDROID OS

Relevant for: Science & Technology | Topic: Computer Technology incl. 3-D Printing

CERT-In detects multiple vulnerabilities in Chrome, Edge browsers and Android OS | Photo Credit: Getty Images

These vulnerabilities can allow remote attackers to execute arbitrary code on the targeted systems compromising their security, CERT-In said.

(Sign up to our Technology newsletter, Today's Cache, for insights on emerging themes at the intersection of technology, business and policy. Click here to subscribe for free.)

Vulnerabilities were detected in Google Chrome versions prior to 104.0.5112.79.

Inappropriate implementation of multiple APIs like Managed Device API, nearby share API, fullscreen and extensions API have led to these vulnerabilities.

An API is a programming interface that allows different software to use features built into the browser.

Vulnerabilities have also been reported in Use after free in Omnibox, Safe Browsing, Tab Strip, Overview Mode, Nearby Share, Input, Sign-In Flow, WebUI, and Insufficient policy enforcement in Background Fetch and Cookies.

In Android OS, vulnerabilities have been reported in versions 10, 11, 12 and 12L.

These vulnerabilities exist due to flaws in the existing framework of the software, Google play system, imagination technologies among others. These can allow attackers to access privileged information in Android OS smartphones, CERT-In said.

In Microsoft Edge, vulnerabilities were detected in versions prior to 104.0.1293.47.

Attackers can exploit these vulnerabilities to bypass security restrictions in the browser and access privileged resources in the affected systems. They can then use that to escape the sandbox of the browser and target other areas of the compromised systems, according to CERT-In.

Our code of editorial values

END