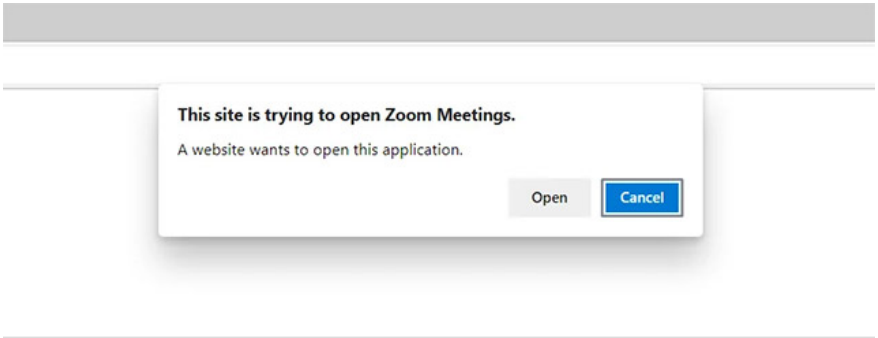
Vulnerabilities discovered in many web browsers that allow users to be tracked through installed applications

International security researchers have recently developed a method, or rather, a rather dangerous new vulnerability on many popular web browsers.

If successfully exploited, the vulnerability could allow a malicious actor to track a specific user across multiple browser platforms on the same device by querying the very apps the target has installed. placed on that device.

In fact, certain apps, when installed, create a custom URL scheme that the browser can use to launch URLs in those specific apps.

For example, the custom URL scheme for the popular online conferencing application Zoom is zoommtg:// which, when opened, prompts the browser to launch the Zoom client, as shown in the illustration below. .



There are over a hundred different custom URL handlers configured by the apps, including many well-known names like Slack, Skype, Spotify, Zoom, vscode, Epic Games, Telegram, Discord, Slack , Steam, Battle.net, Xcode, NordVPN, Sketch, Teamviewer, Microsoft Word, WhatsApp, Postman, Adobe, Messenger, Figma, Hotspot Shield, ExpressVPN, Notion or even iTunes.

Browser tracking using URL scheme

A team of security researchers from FingerprintJS recently found a vulnerability that allows websites to track users across many different browsers, including popular names like Chrome, Firefox, Microsoft Edge , Safari and even Tor.

To perform cross-browser tracking by taking advantage of the URL scheme, a website would have to build a profile of the apps installed on the target's device by attempting to open handlers Their known URL, and

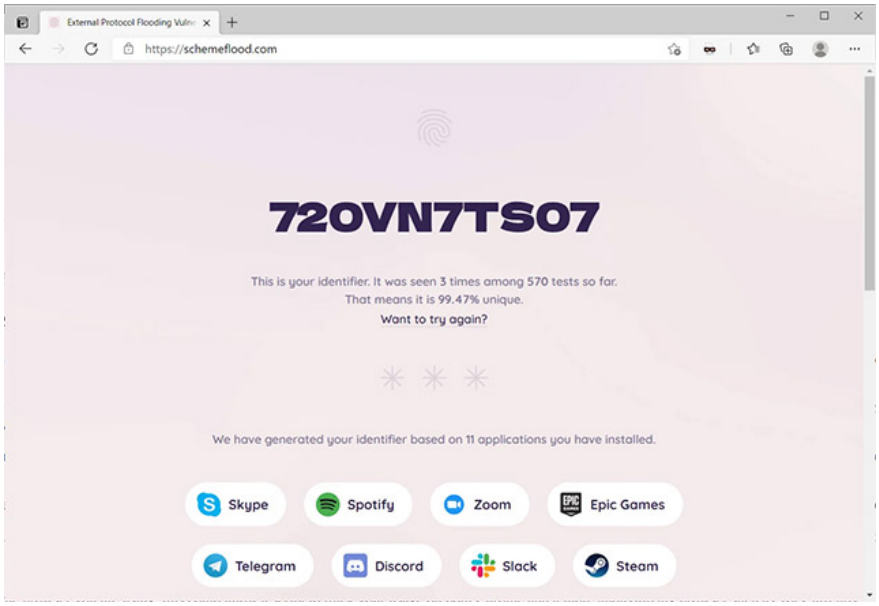
especially check if the browser launches the prompt.

If a prompt is given to open the application, it can be assumed that a particular application is already installed. By testing different URL handlers, a script can use detected apps to create a unique profile for your device.

Since the apps installed on the device don't change no matter what browser you're using, this could allow the script to track the user's browser usage on both Google Chrome and the hidden browser name like Tor.

To test this vulnerability, researchers at BleepingComputer tried accessing a demo website at Schemeflood.com with Microsoft Edge - where a script launches URL handlers for multiple applications to determine if they installed or not.

The results showed that a unique identifier was displayed on the user's profile. In particular, this identifier is completely null for tests using other browsers such as Firefox, Google Chrome and Tor. This is the code that websites can use to track users.



Notably, out of the four major browsers tested, only Google Chrome has added mitigations to prevent this type of attack. Specifically by preventing multiple attempts to use URL handlers without user action (interaction). However, researchers have also found that activating a built-in Chrome extension, such as PDF Viewer, bypasses this mitigation effort.

In related news, Microsoft Edge program manager Eric Lawrence acknowledged the existence of this attack, and said that Chromium and Microsoft engineers are actively working on fixing the bug.

You finished reading the article "**Vulnerabilities discovered in many web browsers that allow users to be tracked through installed applications**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.