El navegador de código abierto Tor, se actualizó a la versión 10.0.18 con correcciones para distintos problemas, incluyendo un error que elimina la privacidad que podría usarse para huellas dactilares de usuarios en diferentes navegadores según las aplicaciones instaladas en una computadora.

Además de la actualización de Tor a la versión 0.4.5.9 para Android, se actualizó Firefox a la versión 89.1.1, aparte de incorporar parches implementados por Mozilla para varias vulnerabilidades de seguridad que fueron abordadas en Firefox 89.

El principal de los problemas corregidos se refiere aun ataque de huellas dactilares que salió a la luz el mes pasado. Conocida como inundación de esquemas, la vulnerabilidad permite que un sitio web malicioso aproveche la información sobre las aplicaciones instaladas en el sistema para asignar a los usuarios un identificador único permanente incluso cuando cambian de navegador, usan el modo de incógnito o una VPN.

En otras palabras, la vulnerabilidad se aprovecha de los esquemas de URL personalizados en las aplicaciones como un vector de ataque, lo que permite a un mal actor rastrear al usuario de un dispositivo entre diferentes navegadores, incluidos Chrome, Firefox, Microsoft Edge, Safari e incluso Tor, eludiendo de forma efectiva entre los navegadores las protecciones de anonimato en Windows, Linux y MacOS.

> *«Un sitio web que explote la vulnerabilidad de inundación del esquema podría crear un identificador estable y único que pueda vincular esas identidades de navegación»,* dijo Konstantin Darutkin, investigador de FingerprintJS.

Actualmente, el ataque verifica una lista de 24 aplicaciones instaladas que consta de Adobe, Battle.net, Discord, Epic Games, ExpressVPN, Facebook Messenger, Figma, Hotspot Shield, iTunes, Microsoft Word, NordVPN, Notion, Postman, Sketch, Skype, Slack, Spotify, Steam, TeamViewer, Telegram, Visual Studio Code, WhatsApp, Xcode y Zoom.

El problema tiene serias implicaciones para la privacidad, ya que los atacantes podrían

aprovecharlo para desenmascarar a los usuarios de Tor al correlacionar sus actividades de navegación cuando cambian a un navegador no anonimizado, como Google Chrome. Para contrarrestar el ataque, Tor ahora establece *«network-protocol-handler.external»* en falso para evitar que el navegador pruebe las aplicaciones instaladas.

De los otros tres navegadores, aunque Google Chrome presenta protecciones integradas contra la inundación de esquemas (evita el inicio de cualquier aplicación a menos que sea activada por un gesto del usuario, como un clic del mouse), se encontró que el Visor de PDF del navegador elude esta mitigación.

> *«Hasta que se solucione esta vulnerabilidad, la única forma de tener sesiones de navegación privada no asociadas con su dispositivo principal es usar otro dispositivo por completo»,* dijo Darutkin.

Se recomienda a los usuarios de Tor que apliquen la actualización lo más rápido posible para asegurarse de estar protegidos.

El desarrollo surge a poco más de una semana después de que el servicio de mensajería cifrada Wire solucionó dos vulnerabilidades críticas en su aplicación web y de iOS, que podrían conducir a una denegación de servicio (CVE-2021-32666) y permitir que un atacante tome el control de una cuenta de usuario (CVE-2021-32683).