Vulnerabilidad De WebRTC Filtra Las Direcciones IP Reales De Los Usuarios De VPN

Se ha encontrado una **vulnerabilidad De WebRTC** (Web Real-Time Communication), un estándar de código abierto que permite a los navegadores web realizar llamadas de voz o de vídeo sin necesidad de ningún tipo de complementos o extensión.

Aplicaciones Afectadas

A finales del mes pasado, investigadores de seguridad revelaron una **vulnerabilidad de seguridad** que permite al propietario del sitio web ver fácilmente las direcciones IP reales de los usuarios que usan el **servicio de WebRTC**, incluso si están utilizando una VPN o incluso PureVPN para cubrir su dirección IP real.

El fallo de seguridad afecta a los navegadores que tienen soporte de WebRTC, como Google Chrome y Mozilla Firefox, y parece estar limitado al sistema operativo de Windows, aunque los **usuarios de Linux y Mac OS X** no están afectados por esta vulnerabilidad.

¿Como Funciona La Falla En WebRTC?

WebRTC permite que las solicitudes a realizar para Servidores STUN (Session Traversal Utilities for NAT) que devuelven la dirección IP «oculta» de donde proviene la conexión, así como las direcciones de red locales para el

sistema que está siendo utilizadas por el usuario.

Los resultados de las solicitudes se puede acceder mediante JavaScript, pero, al realizarse fuera del procedimiento de solicitud XML/HTTP normal, no son visibles desde la consola de desarrollador.

Comprueba El Fallo

Una demostración ha sido publicada por el desarrollador Daniel Roesler en GitHub, el cual permite a las personas comprobar si son afectados por la falla de seguridad.

También, puedes usar los siguientes pasos para comprobar si eres vulnerable al fallo:

- Conectarse a ExpressVPN
- Visita

- Si tu navegador es seguro, deberás ver algo como lo anterior.
- Si tu navegador está afectado por este problema, verás información acerca de la verdadera dirección IP en la sección WebRTC.

Cómo Protegerse

Por suerte, el fallo de seguridad crítico es **bastante fácil de solucionar**.

Para los usuarios de Chrome:

Google Chrome y otros usuarios de navegadores basados en Chromium pueden instalar la extensión WebRTC Block o ScriptSafe, los cuales pueden bloquear la vulnerabilidad.

Para los usuarios de Firefox:

En el caso de Firefox, puedes usar NoScript. Para solucionarlo, pruebe los siguientes pasos:

- Escriba about: config en la barra de direcciones del navegador y pulse intro.
- Confirma que será cuidado si aparece el símbolo.
- Busca **media.peerconnection.enabled**.
- Haga doble clic en la preferencia para definirla con false.
- Y listo!