WhatsApp Web: cuatro fallas en la app pusieron en riesgo los celulares de los usuarios

07/02/2020

Cuatro fallos de seguridad críticos en la versión para computadoras de la aplicación de mensajería WhatsApp expusieron los dispositivos de los usuarios, a los que un atacante podía acceder a través del envío de un mensaje malicioso.

Las vulnerabilidades, que fueron descubiertas por los investigadores de la compañía de ciberseguridad Perimeter X, se basan en el «cross-site scripting», un agujero de seguridad que permite a un tercero inyectar código Javascript o similar en una aplicación web.

En WhatsApp, cuando el usuario envía un mensaje que contiene un enlace, la aplicación añade una previsualización con información adicional, como el nombre de la página y su descripción, para que el receptor sepa dónde está haciendo click. No obstante, estos datos provienen del emisor del mensaje y pueden alterarse de forma malintencionada.

Aprovechándose de esto, un atacante podría utilizar un mensaje malicioso modificado, pero con apariencia de legítimo, cambiar la URL del enlace e introducir código malicioso Java escondido a través del «cross-site scripting».

Mediante esta técnica, el atacante puede hacerse con acceso a los archivos del sistema de WhatsApp y ejecutar código de forma arbitraria en el dispositivo a través de la aplicación del usuario que reciba el chat malicioso.

Este fallo está presente solo en algunos navegadores como en Safari y en versiones antiguas de Edge, pero no en otros

basados en Chromium, según la investigación, y se debe al uso en WhatsApp de la herramienta de desarrollo de aplicaciones Electron, basada en versiones antiguas de Chromium aún afectadas por el problema.

Tras descubrir estas vulnerabilidades, los investigadores de Perimeter X le informaron a Facebook, compañía propietaria de WhatsApp desde 2014, y estos fallos fueron solucionados a través de un parche de seguridad en WhatsApp Web para PC y Mac distribuido el pasado 21 de enero.

Fuente: TN