Un investigador de seguridad reveló hoy los detalles técnicos de múltiples vulnerabilidades de alta gravedad en WhatsApp, que de ser explotadas, podrían haber permitido que hackers remotos comprometan la seguridad de miles de millones de usuarios de distintas formas.

Al combinarse, los problemas informados podrían haber permitido a los piratas informáticos robar remotamente archivos de computadoras Windows o Mac mientras las víctimas utilizan la aplicación de escritorio de WhatsApp.

Gal Weizman, de PerimeterX, es el investigador que descubrió las vulnerabilidades, bajo el identificador CVE-2019-18462, los defectos residían específicamente en WhatsApp Web, una versión de navegador de la aplicación de mensajería.

En una publicación de blog, Weizman reveló que WhatsApp Web era vulnerable a una falla de redirección abierta potencialmente peligrosa que condujo a ataques persistentes de secuencias de comandos entre sitios, que podrían haberse desencadenado al enviar un mensaje especialmente diseñado a los usuarios de WhatsApp específicos.

En caso de que la víctima desprevenida vea el mensaje malicioso en su navegador web, la falla podría haber permitido que el atacante ejecute código arbitrario en el contexto del dominio web de WhatsApp.

Por otro lado, al ver por medio de la app de escritorio vulnerable, el código malicioso se ejecuta en los sistemas de los destinatarios en el contexto de la aplicación vulnerable.

Además, la política de seguridad de contenido mal configurada en el dominio web de WhatsApp también permitió al investigador cargar cargas útiles de XSS de cualquier longitud mediante un iframe de un sitio web controlado por el atacante en Internet.

> *«Si las reglas de CSP estuvieran bien configuradas, la potencia obtenida por este XSS habría sido mucho menor. Ser capaz de eludir la configuración de CSP le permite a un atacante robar información valiosa de la víctima, cargar fácilmente*

> *cargas útiles externas y mucho más»*, dijo el investigador.

Como se muestra en la captura de pantalla, Weizman demostró el ataque remoto de lectura de archivos por medio de WhatsApp accediendo al contenido del archivo de hosts desde la computadora de la víctima.

Además, la falla de redireccionamiento abierto también podría haberse utilizado para manipular los banners de URL, una vista previa del dominio que WhatsApp muestra a los destinatarios cuando reciben un mensaje que contiene enlaces, y engañar a los usuarios para que caigan en ataques de phishing.

Weizman informó responsablemente los problemas al equipo de seguridad de Facebook el año pasado, mismo que corrigió las fallas y lanzó una versión actualizada de su aplicación de escritorio y también recompensó a Weizman con 12,500 dólares bajo el programa de recompensas por errores de la compañía.