La semana pasada se reportó que Microsoft lanzó una versión actualizada de su aplicación Outlook para Android, que corrige una grave vulnerabilidad de ejecución remota de código (CVE-2019-1105), que afectó a más de 100 millones de usuarios.

Sin embargo, hasta ahora muy pocos detalles sobre el fallo estaban disponibles en su aviso, que reveló que las versiones anteriores de la app de correo electrónico contenían una falla de scripts entre sitios (XSS) que permitía a los hackers ejecutar scripts en el contexto del usuario actual simplemente al enviar un correo electrónico especialmente diseñado para las víctimas.

Bryan Appleby, de F5 Networks, uno de los investigadores de seguridad que informó sobre este problema de manera independiente a Microsoft, presentó más detalles y prueba de concepto de la vulnerabilidad de Outlook que informó al gigante de la tecnología hace casi seis meses.

En una publicación el viertes, Appleby reveló que mientras intercambiaba un código JavaScript con sus amigos por medio de correo electrónico, descubrió accidentalmente un problema de scripts entre sitios (XSS) que podía permitir que un atacante incrustara un iframe en el correo electrónico.

Esto significa que la vulnerabilidad reside en la forma en que el servidor de correo electrónico analiza las entidades HTML en los mensajes de correo electrónico.

Aunque el JavaScript que se ejecuta dentro de un iframe solo puede acceder al contenido dentro de él, Appleby descubrió que la ejecución del código JavaScript dentro del iframe inyectado puede permitir que el atacante lea contenido relacionado con la aplicación en el contexto del usuario de Outlook registrado, incluyendo sus cookies, tokens y algunos contenidos de su bandeja de entrada de correo electrónico.

La vulnerabilidad, según Appleby, le permitió *«robar datos de la aplicación, podría usarla para leer y extraer el HTML».*

> *«Este tipo de vulnerabilidad podría ser explotada por un atacante que envía un correo electrónico con JavaScript. El servidor escapa de ese JavaScript y no lo ve porque está dentro de un iframe. Cuando se entrega, el cliente de correo deshace automáticamente el escape, y el JavaScript se ejecuta en el dispositivo cliente. Bingo, ejecución remota de código»*, explicó Appleby.
>
> *«Este código puede hacer lo que desee el atacante, hasta el robo de información y/o envío de datos. Un atacante puede enviar un correo electrónico y, al ser leído por la víctima, el atacante puede robar el contenido de su bandeja de entrada. Puede convertirse en una pieza de malware muy desagradable»*, agregó.

Appleby informó sobre esto a Microsoft el 10 de diciembre de 2018, y la compañía confirmó la vulnerabilidad el 26 de marzo de 2019, cuando compartió un PoC universal.

Microsoft parcheó la vulnerabilidad y lanzó una solución hace dos días, eso es casi seis meses después de la divulgación de la vulnerabilidad inicial. La compañía asegura que actualmente no tiene conocimiento de ningún ataque en la naturaleza relacionado con el problema.

Aparte de Appleby, los investigadores de seguridad Sander Vanrapenbush, Tom Wyckhuys, Eliraz Duek de CyberArk y Gaurav Kumar, también informaron el mismo problema a Microsoft por separado en los últimos meses.