Si utilizas un teléfono inteligente Mi o Redmi de Xiaomi, debes dejar de utilizar inmediatamente el navegaador MI integrado o el navegador Mint disponible en Google Play Store para dispositivos Android que no sean Xiaomi.

Esto se debe a que las dos aplicaciones de navegador web creadas por Xiaomi son vulnerables a un fallo crítico que no ha sido reportado aún, incluso después de haber sido informada de forma privada a la compañía.

La vulnerabilidad, identificada como CVE-2019-10875 y descubierta por el investigador de seguridad Arif Khan, es un problema de suplantación de la barra de direcciones del navegador originada debido a una falla lógica en la interfaz del navegador, lo que permite que un sitio web malintencionado controle las URL que se muestran en la barra de direcciones.

De acuerdo con el aviso, los navegadores afectados no manejan correctamente el parámetro de consulta *«q»* en las URL, por lo que no muestran la parte de una URL https antes de la subcadena *?q=* en la barra de direcciones.

Como la barra de direcciones de un navegador web es el indicador de seguridad más confiable y esencial, la falla se puede utilizar para engañar fácilmente a los usuarios de Xiaomi para que piensen que están visitando un sitio web de confianza cuando en realidad se les está proporcionando un contenido malicioso mediante phishing, como se muestra en el video a continuación.

Los ataques de phishing en la actualidad son más sofisticados y cada vez más difíciles de detectar, y esta vulnerabilidad de suplantación de URL lo lleva a otro nivel, lo que le permite a uno evitar indicadores básicos como URL y SSL, que son las primeras cosas que cualquier usuario verifica para determinar si un sitio web es falso.

The Hacker News verificó de forma independiente la vulnerabilidad utilizando un PoC que el investigador compartió con el equipo, y pudo confirmar que funciona en las últimas versiones de ambos navegadores web: Mi Browser (v10.5.6-g) y Mint Browser (v1.5.3), que están

disponibles en el momento de la escritura.

Algo curioso es que el problema solo afecta a las variantes internacionales de ambos navegadores web, aunque las versiones domésticas, distribuidas con los teléfonos inteligentes Xiaomi en China, no cuentan con esa vulnerabilidad.

> *«Lo que más me llamó la atención fue que solo sus versiones en el extranjero o internacional tenían este error de seguridad y no sus versiones en chino o nacional. ¿Se hizo de forma deliberada? ¿Los fabricantes chinos de dispositivos hacen que sus sistemas operativos, aplicaciones y firmware sean intencionalmente vulnerables para sus usuarios internacionales?»*, dijo Arif.

Otra peculiaridad es que al informar el problema, Xiaomi recompensó al investigador con una llamada *«recompensa de errores»,* pero dejó la vulnerabilidad sin parchear.

> *«La vulnerabilidad afecta a millones de usuarios en todo el mundo, pero la recompensa ofrecida como tal fue de $99 dólares (para Mi Browser) y otros $99 dólares para Mint Browser»,* dijo el investigador.

También contactamos con Xiaomi dos días antes de publicar este informe para obtener comentarios adicionales y saber si la compañía tiene planes de lanzar una versión parcheada en algún momento próximo, pero el proveedor de servicios móviles proporcionó una respuesta rara.

> *«Me gustaría informarle que a partir de ahora no hay una actualización oficial sobre el tema. Sin embargo, le solicitaré que se mantenga conectado con la página del foro para obtener más detalles al respecto»,* dijo la compañía.

Este es el segundo problema grave revelado que los investigadores identificaron en aplicaciones preinstaladas en más de 150 millones de dispositivos Android fabricados por Xiaomi.

Apenas ayer se publicaron detalles de un informe que explica cómo los atacantes podrían haber convertido una aplicación de seguridad preinstalada en teléfonos Xiaomi, llamada Guard Provider, en malware al explotar múltiples vulnerabilidades en la aplicación.

Se recomienda a los usuarios de Android que utilicen navegadores web modernos, que no se vean afectados por esta vulnerabilidad, como Chrome o Firefox.

Además, si utilizan el navegador Microsoft Edge o Internet Explorer en escritorio, también es necesario evitar su uso, ya que ambos navegadores también cuentan con esta vulnerabilidad crítica que no ha sido reparada.