En caso de utilizar el navegador web Firefox para Android, es necesario asegurarse de que se haya actualizado a la versión 80 o posterior disponible en Google Play Store, para evitar problemas de seguridad.

El investigador de seguridad cibernética de ESET, Lukas Stefanko, advirtió sobre una vulnerabilidad de ejecución remota de comandos de alto riesgo recientemente revelada, que afecta a la aplicación Firefox para Android.

Descubierta originalmente por el investigador de seguridad australiano Chris Moberly, la vulnerabilidad reside en el motor SSDP del navegador, que puede ser explotado por un atacante para apuntar a teléfonos inteligentes Android conectados a la misma red WiFi que el atacante, con la aplicación Firefox instalada.

SSDP, que son la siglas de Simple Service Discovery Protocol, es un protocolo basado en UDP que forma parte de UPnP para encontrar otros dispositivos en una red. En Android, Firefox envía de forma periódica mensajes de descubrimiento SSDP a otros dispositivos conectados a la misma red, buscando dispositivos de segunda pantalla para transmitir.

Cualquier dispositivo de la red local puede responder a estas transmisiones y proporcionar una ubicación para obtener información detallada en un dispositivo UPnP, después de lo cual, Firefox intenta acceder a esa ubicación, esperando encontrar un archivo XML que cumpla con las especificaciones UPnP.

Según el informe de vulnerabilidad que Moberly envió al equipo de Firefox, se puede engañar al motor SSDP de los navegadores Firefox de las víctimas para que active un intent de Android simplemente reemplazando la ubicación del archivo XML en los paquetes de respuesta con un mensaje especialmente diseñado que apunta a un intent URI de android.

Para esto, un atacante conectado a una red WiFi específica, puede ejecutar un servidor SSDP malicioso en su dispositivo y activar comandos basados en el intent de dispositivos Android cercanos a través de Firefox, sin requerir ninguna interacción de las víctimas.

Las actividades permitidas por el intent también incluyen el inicio automático del navegador y la apertura de cualquier URL definida, lo que, según los investigadores, es suficiente para engañar a las víctimas para que proporcionen sus credenciales, instalen aplicaciones maliciosas, entre otras actividades basadas en escenarios circundantes.

> *«El objetivo simplemente debe tener la aplicación Firefox ejecutándose en su teléfono. No necesita acceder a sitios web maliciosos ni hacer clic en ningún enlace. No se requiere la instalación de una aplicación maliciosa o atacante en el medio. Simplemente pueden estar bebiendo café mientras está en el WiFi del establecimiento, y el dispositivo comenzará a lanzar la URI de la aplicación bajo el control del atacante»,* dijo Moberly.
>
> *«Podría haber sido usado de una forma similar a los ataques de phishing donde un sitio malicioso es forzado al objetivo sin su conocimiento con la esperanza de que ingresen información confidencial o acepten instalar una aplicación maliciosa»,* agregó.

Moberly informó sobre la vulnerabilidad al equipo de Firefox hace algunas semanas, y el fabricante del navegador ya corrigió el problema en las versiones 80 y posteriores de Firefox para Android.

El investigador también lanzó un exploit de prueba de concepto al público que Stefanko usó para demostrar el problema en el video anterior con tres dispositivo conectados a la misma red WiFi.