UC Browser se salta las normas de Google Play y puede descargar código de servidores externos, según Dr. Web

Navegadores en Google Play hay muchos. Puede que el más popular sea Google Chrome, pero hay alternativas como Firefox, el navegador de Samsung y UC Browser, desarrollado por UCWeb. Este acumula en su haber más de 500 millones de descargas y no ha estado exento de polémica. El año pasado fue retirado de la tienda por un supuesto "error no intencionado" relacionado con algunas medidas tomadas para aumentar las instalaciones, y ahora vuelve a estar en el punto de mira por saltarse las normas de Google Play.

Según ha descubierto Dr. Web, UC Browser tiene una "función oculta para descargar y ejecutar código cuestionable en dispositivos móviles". Aparentemente, el navegador puede descargar módulos adicionales desde servidores de terceros para añadir funciones o actualizarse, "lo que supone una seria amenaza porque permite ejecutar código, también malicioso, en dispositivos Android".

Desde Dr.Web destacan que, durante su análisis, UC Browser descargó una librería de un servidor externo que, si bien no era maliciosa, se guardó en su directorio y se ejecutó. Esta función ha estado presente “al menos desde 2016” y parece que, por ahora, no se ha usado nunca para descargar malware o código malicioso.

Sin embargo, abre las puertas a que se puedan hacer ataques MITM (man in the middle), ya que no se usa una conexión segura para conectar con los servidores. Para descargar los módulos, el navegador manda una solicitud al servidor y recibe un link para descargarlo, todo ello usando el protocolo HTTP en lugar de HTTPS, es decir, que la conexión no está encriptada. Eso permitiría a cualquier persona con los conocimientos adecuados interceptar la transferencia y reemplazar el código. Para más inri, los módulos de UC Browser no están firmados, por lo que el módulo infectado se podría ejecutar sin ser verificado.

Para ponerlo a prueba, los chicos de Dr. Web ejecutaron un ataque MITM que puedes ver más arriba. Para ello, descargaron una archivo PDF que requería que UC Browser descargase un módulo adicional para poder abrirlo. Interceptaron la conexión

y sustituyeron la librería por una nueva que creaba un mensaje de texto en el que se puede leer “PWNED!”.

En la política de privacidad de Google Play se establece que no se permiten “aplicaciones que instalen otras aplicaciones en un dispositivo sin el consentimiento previo del usuario” o que “descarguen código ejecutable, como archivos dex o código nativo, de una fuente que no sea Google Play”. AnTuTu, por ejemplo, debe descargar el módulo para el benchmark 3D para poder completar el análisis, pero lo hace desde Google Play, no desde una fuente ajena a la tienda de aplicaciones.

Tanto UC Browser como UC Browser Mini pueden descargar módulos de fuentes externas a Google Play
Según Dr. Web, esta política se aplicó para “prevenir la distribución de troyanes moduladores” como pudieron ser Android.RemoteCode.127.Origin y Android.RemoteCode.152.origin, descubiertos en enero y abril del año pasado. Cabe destacar que esta función de descarga se ha descubierto tanto en UC Browser como UC Browser Mini (que tiene 100 millones de descargas). La compañía se ha negado a hacer comentarios al respecto, por lo que Dr. Web ha puesto el caso en conocimiento de Google. Por el momento, ambas aplicaciones siguen en la tienda.

Fuente: xatakandroid.