NSO Group, el grupo desarrollador del malware Pegasus, nuevamente es noticia, esta vez por explotar una vulnerabilidad crítica de día cero sin parches en el sistema operativo Android.

La vulnerabilidad descubierta por el investigador del Project Zero, Maddie Stone, los detalles y un exploit de prueba de concepto para la vulnerabilidad de seguridad grave, rastreada como CVE-2019-2215, se hicieron públicos hoy, a solo siete días después de informar sobre esto al equipo de seguridad de Android.

El 0-day en cuestión es una vulnerabilidad sin uso en el controlador de carpeta del kernel de Android que puede permitir que un atacante privilegiado local o una aplicación, escale sus privilegios para obtener acceso root a un dispositivo vulnerable y potencialmente tomar el control remoto completo del dispositivo.

Dispositivos Android vulnerables

La vulnerabilidad reside en las versiones del kernel de Android lanzadas antes de abril del año pasado, un parche que se incluyó en el kernel 4.14 LTS Linux lanzado en diciembre de 2017, pero solo se incorporó en las versiones 3.18, 4.4 y 4.9 del kernel de android AOSP.

Por lo tanto, la mayoría de los dispositivos Android fabricados y vendidos por la mayoría de los proveedores con el núcleo no parcheado aún son vulnerables a este problema incluso después de tener las últimas actualizaciones de Android, incluyendo los modelos de smartphones populares como los siguientes:

- Pixel 1
- Pixel 1 XL
- Pixel 2
- Pixel 2 XL
- Huawei P20
- Xiaomi Redmi 5A
- Xiaomi Redmi Note 5
- Xiaomi A1

- Oppo A3
- Moto Z3
- Oreo LG
- Samsung S7
- Samsung S8
- Samsung S9

El Pixel 3, 3 XL y 3a que corren la última versión del kernel de Android no son vulnerables a este problema.

La falla de Android se puede explotar remotamente

Según el investigador, ya que el problema es *«accesible desde el interior del entorno limitado de Chrome»,* la vulnerabilidad de día cero del kernel de Android también se puede explotar remotamente, al combinarla con un defecto de representación de Chrome por separado.

> *«El error es una vulnerabilidad de escalada de privilegios locales que permite un compromiso total de un dispositivo vulnerable. Si el exploit se entrega por medio de la web, solo se necesita ser emparejado con un exploit de renderizador, ya que esta vulnerabilidad es accesible por medio del sandbox»,* dijo Stone en el blog Chromium.
>
> *«He adjuntado una prueba de concepto de explotación local para demostrar cómo se puede utilizar este error para obtener lectura/escritura arbitraria del núcleo cuando se ejecuta localmente. Solo requiere la ejecución de código de aplicación no confiable para explotar CVE-2019-2215. También adjunté una captura de pantalla (success.png) del PoC que se ejecuta en un Pixel 2, con Android 10 con nivel de parche de seguridad en septiembre de 2019».*

Aunque Google lanzará un parche para esta vulnerabilidad en su Boletín de Seguridad de

Android de octubre en los siguientes días, y también notificó a los OEM, la mayoría de los dispositivos afectados probablemente no recibirán el parche inmediatamente, a diferencia del Google Pixel 1 y 2.

> *«Este problema está calificado como de alta gravedad en Android y por sí solo requiere la instalación de una aplicación maliciosa para su posible explotación. Cualquier otro vector, como por medio del navegador web, requiere encadenarse con un exploit adicional. Hemos notificado a los socios de Android y el parche está disponible en el kernel común de Android. Los dispositivos Pixel 3 y 3a no son vulnerables, mientras que los dispositivos Pixel 1 y 2 recibirán actualizaciones para este problema como parte de la actualización de octubre»,* dijo el investigador.

La división Project Zero de Google generalmente le brinda a los desarrolladores de software una fecha límite de 90 días para solucionar el problema en sus productos afectados antes de hacer públicos los detalles y las vulnerabilidad de PoC, pero en caso de vulnerabilidades activas, el equipo de hace público después de siete días de denuncia privada.

Aunque la vulnerabilidad es grave y se puede utilizar para obtener acceso de root en un dispositivo Android, los usuarios no deben preocuparse demasiado, pues la explotación de estos problemas se limita principalmente a escenarios de ataques dirigidos.