Alerta de seguridad informática	9VSA-00097-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de diciembre de 2019
Última revisión	8 de diciembre de 2019

NOTIFICACIÓN
La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de Android, referente a vulnerabilidades que afectan su sistema operativo. De ser explotadas, estas pueden resultar en múltiples ataques, como exposición de información sensible, denegación de servicios permanente, ejecución de código remoto, entre otros. Junto a este informa se publican las respectivas actualizaciones para mitigar los riesgos.

Vulnerabilidad

Parche de seguridad nivel 01-12-2019

Framework:
CVE-2019-2232
CVE-2019-9464
CVE-2019-2217
CVE-2019-2218
CVE-2019-2220
CVE-2019-2221

Media framework:
CVE-2019-2222
CVE-2019-2223

Sistema:
CVE-2019-2224

CVE-2019-2225
CVE-2019-2226
CVE-2019-2227
CVE-2019-2228
CVE-2019-2229
CVE-2019-2230

Parche de seguridad nivel 05-12-2019

Framework:
CVE-2019-2219

Sistema:
CVE-2019-2231

Componentes de kernel:
CVE-2018-20961
CVE-2019-15220
CVE-2019-15239

Componentes Qualcomm:
CVE-2019-10557
CVE-2018-11980
CVE-2019-10480
CVE-2019-10481
CVE-2019-10536
CVE-2019-10537
CVE-2019-10595
CVE-2019-10598
CVE-2019-10601
CVE-2019-10605
CVE-2019-10607
CVE-2019-2304

Componentes closed-source Qualcomm:
CVE-2019-2242
CVE-2019-10500
CVE-2019-10525

CVE-2019-10482
CVE-2019-10487
CVE-2019-10516
CVE-2019-2274
CVE-2019-10513
CVE-2019-10517
CVE-2019-10600

Impacto

Parche de seguridad nivel 01-12-2019
Framework: Seis vulnerabilidades subsanadas, las cuales, al ser explotadas, podían exponer información sensible, escalar privilegios, y la más crítica, al enviar un mensaje especialmente diseñado, podía causar una denegación de servicios permanente.

Media framework: Dos vulnerabilidades subsanadas, las cuales, al ser explotadas, permitían la ejecución de código remoto en el contexto de un proceso privilegiado.

Sistema: Siete vulnerabilidades subsanadas, las cuales, al ser explotadas, permitían la escalación de privilegios, exposición de información y ejecución de código remoto en el contexto de un proceso no privilegiado.

Producto Afectado

Dispositivos que utilicen el sistema operativo Android, para conocer su nivel de parche de seguridad, acceder a las siguientes URLs:
Pixel o Nexus:
https://support.google.com/pixelphone/answer/4457705#pixel_phones&nexus_devices
Otros modelos:
https://support.google.com/android/answer/3094742

Mitigación

Se debe actualizar el dispositivo a la última versión disponible, para más información respecto a cómo actualizar, acceder al siguiente URL:

https://support.google.com/android/answer/7680439?hl=en

Enlaces
https://source.android.com/security/bulletin/2019-12-01

Framework:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2232
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-9464

https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2217
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2218
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2220
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2221

Media framework:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2222
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2223

Sistema:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2224
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2225
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2226
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2227
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2228
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2229
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2230

Impacto

Parche de seguridad nivel 05-12-2019
Framework: Una vulnerabilidad subsanada, la cual, al ser explotada, permitía la exposición de información.

Sistema: Una vulnerabilidad subsanada, la cual, al ser explotada, permitía la exposición de información.

Componentes de kernel: Tres vulnerabilidades subsanadas, las cuales, al ser explotadas, permitían la escalación de privilegios en el sistema.

Componentes Qualcomm: Doce vulnerabilidades subsanadas en el componente WLAN host.

Componentes closed-source Qualcomm: Diez vulnerabilidades subsanadas.

Producto Afectado

Dispositivos que utilicen el sistema operativo Android, para conocer su nivel de parche de seguridad, acceder a las siguientes URLs:

Pixel o Nexus:
https://support.google.com/pixelphone/answer/4457705#pixel_phones&nexus_devices

Otros modelos:
https://support.google.com/android/answer/3094742

Mitigación

Se debe actualizar el dispositivo a la última versión disponible, para más información respecto a cómo actualizar, acceder al siguiente URL:

https://support.google.com/android/answer/7680439?hl=en

Enlaces

https://source.android.com/security/bulletin/2019-12-01

Framework:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2219

Sistema:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2231

Componentes de kernel:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-20961
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-15220
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-15239

Componentes Qualcomm:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-10557
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-11980
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-10480
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-10481
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-10536
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-10537
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-10595
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-10598
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-10601
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-10605
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-10607
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2304

Componentes closed-source Qualcomm:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2242
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-10500
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-10525
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-10482
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-10487
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-10516
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-2274
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-10513
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-10517
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-10600

Las actualizaciones de seguridad liberadas para Android por lo general son sólo para los dispositivos de Google (Nexus y Pixel), sin embargo las demás marcas que utilizan el sistema operativo de Android están liberando sus propias versiones de los parches, por lo que se recomienda estar atentos a las actualizaciones e instalarlas inmediatamente cuando estén disponibles.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.12.08 09:19:06 -03'00'