Alerta de seguridad informática	9VSA-00065-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de octubre de 2019
Última revisión	10 de octubre 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 la información entregada por Android en su boletín mensual de Octubre, parchando un total de 26 vulnerabilidades, 8 de las cuales han sido catalogadas como críticas y 16 de ellas como altas. Estas son de tipo ejecución de código remoto, escalación de privilegios, exposición de información, denegación de servicios, entre otras.

Vulnerabilidades

- CVE-2019-2110
- CVE-2019-2114
- CVE-2019-2173
- CVE-2019-2184
- CVE-2019-2185
- CVE-2019-2186
- CVE-2019-2187
- CVE-2019-2215
- CVE-2019-2251
- CVE-2019-2268
- CVE-2019-2271
- CVE-2019-2289
- CVE-2019-2295
- CVE-2019-2303
- CVE-2019-2315
- CVE-2019-2318
- CVE-2019-2329
- CVE-2019-2335
- CVE-2019-2336
- CVE-2019-2339
- CVE-2019-10490
- CVE-2019-10513
- CVE-2019-10535
- CVE-2019-11902
- CVE-2019-13916
- CVE-2019-19824

Productos Afectados

Dispositivos con SO Android.
Estas vulnerabilidades afectan a diferentes componentes en los dispositivos Android, estos son: Framework, Media Framework, System, Google Play System, Kernel, Qualcomm y Qualcomm closed-source.

Mitigaciones

Aplicar las actualizaciones publicadas por el fabricante dependiendo del Security patch level de su dispositivo, para más información respecto a cómo actualizar, visitar segundo y tercer enlace.

Enlaces

- https://source.android.com/security/bulletin/2019-10-01
- https://source.android.com/security/enhancements/enhancements60
- https://support.google.com/pixelphone/answer/4457705#pixel_phones&nexus_devices
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2110
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2114
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2173
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2184
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2185
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2186
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2187
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2215
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2251
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2268
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2271
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2289
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2295
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2303
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2315
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2318
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2329
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2335
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2336
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2339
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10490
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10513
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10535
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11902
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13916
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19824

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.10.10 12:50:11 -03'00'