Alerta de seguridad informática	9VSA20-00143-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de febrero de 2020
Última revisión	17 de febrero de 2020

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 de Google, referente a vulnerabilidades que afectan al sistema operativo Android, las cuales de ser explotadas permitirían a un atacante realizar ataques de denegación de servicios, obtener acceso a información sensible, escalar privilegios en el sistema y hasta comprometer completamente al sistema vulnerable. Este informe incluye la respectiva mitigación.

Vulnerabilidades

CVE-2020-0005
CVE-2020-0014
CVE-2020-0015
CVE-2020-0017
CVE-2020-0018
CVE-2020-0020
CVE-2020-0021
CVE-2020-0022
CVE-2020-0023
CVE-2020-0026
CVE-2020-0027
CVE-2020-0028
CVE-2020-0030
CVE-2019-2200

Impactos

CVE-2020-0005

Un atacante remoto podría comprometer completamente al sistema vulnerable, debido a un error de memoria al procesar un input no confiable en “btm_read_remote_ext_features_complete” de “btm_acl.cc” en la funcionalidad Sistema de Android. El atacante podría gatillar un error de escritura fuera de los límites en memoria y ejecutar código arbitrario en el sistema.

CVE-2020-0014

Un atacante local podría escalar privilegios en el sistema afectado, debido a la posibilidad de una aplicación maliciosa utilizar la ventana TYPE_TOAST manualmente y hacerla clickeable en la funcionalidad Framework de Android.

CVE-2020-0015

Un atacante local podría escalar privilegios en el sistema afectado, debido a posibilidad de superponer el diálogo de instalación de certificado con una aplicación maliciosa en “onCreate” de “CertInstaller.Java” en la funcionalidad Framework de Android.

CVE-2020-0017

Un atacante local podría obtener acceso a información potencialmente sensible, por causa de la posibilidad de visibilizar y modificar el diccionario de usuarios primarios por parte de usuarios secundarios en múltiples lugares en la funcionalidad Framework de Android.

CVE-2020-0018

Un atacante local podría obtener acceso a información potencialmente sensible, debido a un error en “MotionEntry::appendDescription” de “InputDispatcher.cpp” en la funcionalidad Framework de Android.

CVE-2020-0020

Un atacante local podría obtener acceso a información potencialmente sensible, debido a un error de lectura fuera de los límites de memoria en la funcionalidad Framework de Android.

CVE-2020-0021

Un atacante remoto podría realizar ataques de denegación de servicios, debido a la ausencia de un paquete en la funcionalidad Framework de Android.

CVE-2020-0022
Un atacante remoto podría comprometer completamente al sistema vulnerable, debido a un error de memoria al procesar un input no confiable en “reassemble_and_dispatch” de “packet_fragmenter.cc” en la funcionalidad Sistema de Android. El atacante podría gatillar un error de escritura fuera de los limites y ejecutar código arbitrario a través de Bluetooth en el sistema.

CVE-2020-0023
Un atacante remoto podría obtener acceso a información potencialmente sensible, debido a la ausencia de un verificador de permisos en “setPhonebookAccessPermission” de “AdapterService.java” en la funcionalidad Sistema de Android. Un atacante podría obtener acceso no autorizado a información sensible si la aplicación maliciosa permite Contactos en Bluetooth.

CVE-2020-0026
Un atacante remoto podría comprometer completamente al sistema vulnerable, debido a un error de uso de memoria luego de liberarla en “Parcel::continueWrite” de “Parcel.cpp” en la funcionalidad Sistema de Android. El atacante podría escalar privilegios en el sistema y comprometerlo completamente.

CVE-2020-0027
Un atacante remoto podría comprometer completamente al sistema debido a un resultado inesperado en “HidRawSensor::batch” de “HidRawSensor.cpp”. El atacante podría generar un error de escritura fuera de memoria y ejecutar código arbitrario el sistema de la víctima.

CVE-2020-0028
Un atacante remoto podría obtener acceso a información potencialmente sensible debido a la posibilidad de evadir configuraciones de DNS privado en “notifyNetworkTested” y funciones relacionadas con “NetworkMonitor.java” en la funcionalidad Sistema de Android.

CVE-2020-0030
Un atacante podría escalar privilegios en el sistema afectado debido a una condición de carrera en “binder_thread_release” de “binder.c”. en el componente “Binder driver” de Android. Un atacante local podría utilizar un archivo especialmente diseñado para explotar la condición de carrera, gatillar un error de uso luego de liberación de memoria y ejecutar código arbitrario con privilegios elevados en el sistema afectado.

CVE-2019-2200
Un atacante local podría escalar privilegios en el sistema afectado debido a la posibilidad de evadir "updatePermissions" en "PermissionManagerService.java". El atacante podría utilizar una aplicación maliciosa para ganar permisos especiales desde otra aplicación y escalar privilegios en el sistema afectado.

Productos afectados
Android versiones 8.0, 8.1, 9 y 10.

Mitigación
Se deben actualizar a las versiones publicadas por el fabricante en el Security Patch Level del 05/02/2020.

Enlaces
https://source.android.com/security/bulletin/2020-02-01
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0005
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0015
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0017
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0018
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0020
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0021
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0023
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0026
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0027
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0028
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0030
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2200

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.02.17 12:32:31 -03'00'