Анализ уязвимостей ПО Android по данным банка ФСТЭК

# Высокий уровень опасности

|  |  |  |  |
| --- | --- | --- | --- |
| Класс уязвимости | Дата выявления | Уровень опаности | Описание уязвимости |
| Уязвимость кода | 07.06.2019 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента NuPlayerCCDecoder.cpp операционной системы Android связана с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код |
| Уязвимость кода | 04.02.2019 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции binder\_alloc\_free\_page (binder\_alloc.c) ядра операционной системы Android связана с повторным освобождением памяти. Эксплуатация уязвимость может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании |
| Уязвимость архитектуры | 03.12.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента HTC Bootloader операционной системы Android связана с ошибками процедуры подтверждения подлинности сертификата. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии |
| Уязвимость кода | 05.11.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость функции vorbis\_book\_decodev\_set (codebook.c) компонента Media Framework операционной системы Android связана с записью за границами буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код |
| Уязвимость кода | 09.10.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции GraphicBuffer::unflatten() (GraphicBuffer.cpp) операционной системы Android связана с ошибками обработки входных данных. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии |
| Уязвимость кода | 01.10.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции sdcardfs\_open (file.c) ядра операционной системы Android связана с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии |
| Уязвимость кода | 01.10.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функций sdcardfs\_create и sdcardfs\_mkdir (inode.c,) ядра операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии |
| Уязвимость кода | 19.09.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции readBytes (xltdecwbxml.c) операционной системы Android вызвана целочисленным переполнением. Эксплуатация уязвимости может позволить нарушителю раскрыть защищаемую информацию с помощью специально созданного запроса |
| Уязвимость кода | 19.09.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции ParsePayloadHeader (payload\_metadata.cc) операционной системы Android связана с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код |
| Уязвимость кода | 17.09.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции l2c\_lcc\_proc\_pdu (l2c\_fcr.cc) операционной системы Android связана с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код |
| Уязвимость кода | 10.09.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции lppTransposer (lpp\_tran.cpp) операционной системы Android связана с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код |
| Уязвимость архитектуры | 31.08.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость приложения SetupWizard операционной системы Android связана с ошибками управления привилегиями. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии |
| Уязвимость кода | 15.08.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции CAacDecoder\_Init (aacdecoder.cpp) операционной системы Android связана с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код |
| Уязвимость кода | 09.08.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции avrc\_msg\_cback (avrc\_api.cc) операционной системы Android связана с чтением за границами буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, раскрыть защищаемую информацию с использованием Bluetooth |
| Уязвимость кода | 08.08.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции bta\_av\_proc\_meta\_cmd (bta\_av\_act.cc) операционной системы Android связана с чтением за границами буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, раскрыть защищаемую информацию с использованием Bluetooth |
| Уязвимость кода | 08.08.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции smp\_process\_keypress\_notification (smp\_act.cc) операционной системы Android связана с чтением за границами буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, раскрыть защищаемую информацию с использованием Bluetooth |
| Уязвимость кода | 08.08.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции smp\_proc\_master\_id (smp\_act.cc) операционной системы Android связана с чтением за границами буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, раскрыть защищаемую информацию с использованием Bluetooth |
| Уязвимость кода | 08.08.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции smp\_proc\_enc\_info (smp\_act.cc) операционной системы Android связана с чтением за границами буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, раскрыть защищаемую информацию с использованием Bluetooth |
| Уязвимость архитектуры | 07.08.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость функции checkGrantUriPermissionLocked (ActivityManagerService.java) компонента Framework операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии с помощью специально созданного файла |
| Уязвимость кода | 07.08.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции mca\_ccb\_hdl\_req (mca\_cact.cc) операционной системы Android связана с чтением данных за границами буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, раскрыть защищаемую информацию с использованием Bluetooth |
| Уязвимость кода | 06.08.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции readMetadata (Utils.cpp) операционной системы Android существует из-за неверного ограничения имени пути к каталогу с ограниченным доступом. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии при подключении USB-устройства |
| Уязвимость архитектуры | 02.08.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции CollectValuesOrEntriesImpl (elements.cc) компонента Framework операционной системы Android связана с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, повысить свои привилегии с помощью специально сформированного файла |
| Уязвимость кода | 31.07.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции AMediaCodecCryptoInfo\_new (NdkMediaCodec.cpp) компонента Framework операционной системы Android связана с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код с помощью специально созданного файла |
| Уязвимость кода | 24.07.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции readVector (iCrypto.cpp) компонента Media framework операционной системы Android вызвана чтением за границами буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, раскрыть защищаемую информацию |
| Уязвимость кода | 16.07.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость менеджера загрузки компонента Framework операционной системы Android связана с недостаточной защитой структуры SQL-запроса. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, раскрыть защищаемую информацию |
| Уязвимость кода | 02.07.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции hid\_debug\_events\_read (drivers/hid/hid-debug.c) операционной системы Android связана с записью за границами буфера. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии |
| Уязвимость кода | 08.06.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции CAacDecoder\_Init (aacdecoder.cpp) операционной системы Android связана с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код |
| Уязвимость кода | 07.06.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции rfc\_process\_mx\_message (rfc\_ts\_frames.cc) службы Bluetooth операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, раскрыть информацию |
| Уязвимость кода | 07.06.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции rfc\_process\_mx\_message (rfc\_ts\_frames.cc) операционной системы Android вызвана чтением данных за границами буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, раскрыть защищаемую информацию |
| Уязвимость кода | 09.05.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции getOffsetForHorizontal (Layout.java) компонента Framework операционной системы Android связана с некорректной зачисткой или освобождением ресурсов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании |
| Уязвимость кода | 07.05.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента Qualcomm Video операционной системы Android вызвана переполнением буфера в памяти. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код |
| Уязвимость кода | 07.05.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость компонента Qualcomm Modem IP Stack операционной системы Android связана с использованием функции assert() или похожего оператора. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании |
| Уязвимость кода | 05.05.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость динамической библиотеки Qualcomm Libgralloc компонента MediaServer операционной системы Android из репозитория CAF связана со смещением указателя за границы выделенной памяти. Эксплуатация уязвимости может позволить нарушителю оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации |
| Уязвимость кода | 05.05.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции csr\_update\_fils\_params\_rso компонента Qualcomm WLAN операционной системы Android из репозитория CAF вызвана целочисленным недополнением. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 05.05.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера IPA компонента Qualcomm Data Network Stack & Connectivity операционной системы Android из репозитория CAF связана с использованием памяти после её освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 05.05.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера Qualcomm WLAN операционной системы Android из репозитория CAF вызвана переполнением буфера в стеке. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 05.05.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера Qualcomm WLAN операционной системы Android из репозитория CAF вызвана переполнением буфера в «куче». Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 05.05.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции lim\_send\_sme\_probe\_req\_ind компонента Qualcomm WLAN операционной системы Android из репозитория CAF вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 01.05.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента NVIDIA Tegra X1 TZ операционной системы Android вызвана записью данных за пределами буфера в памяти. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии |
| Уязвимость кода | 01.05.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента NVIDIA Trusted Execution Environment (TEE) операционной системы Android связана с повреждением памяти при спекулятивном выполнении TEE . Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии |
| Уязвимость кода | 05.04.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции ipSecSetEncapSocketOwner (XfrmController.cpp) операционной системы Android связана с ошибками при освобождении ресурсов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании |
| Уязвимость кода | 05.04.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции copy\_process ядра операционной системы Android вызвана повторным освобождением памяти. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии |
| Уязвимость кода | 01.04.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость компонента Qualcomm операционной системы Android связана с ошибками в работе сторожевого таймера. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании |
| Уязвимость кода | 05.03.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента NVIDIA Libnvomx операционной системы Android связана с записью за границами буфера в памяти. Эксплуатация уязвимости может позволить нарушителю повысить привилегии |
| Уязвимость кода | 05.03.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента NVIDIA Libnvomx операционной системы Android связана с недостаточной проверкой вводимых данных. Эксплуатация уязвимости может позволить нарушителю повысить привилегии |
| Уязвимость кода | 05.03.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции oem\_cmd\_handler компонента WLAN операционной системы Android из репозитория CAF связана с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, раскрыть защищаемую информацию с использованием специально сформированного запроса |
| Уязвимость кода | 01.02.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость компонента audioserver операционной системы Android связана с записью данных за границами буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, раскрыть защищаемую информацию |
| Уязвимость кода | 19.01.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента Qualcomm Biometrics операционной системы Android вызвана переполнением буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, выполнить произвольный код |
| Уязвимость архитектуры | 11.01.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость компонента Media Framework (AACExtractor.cpp) операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 03.01.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента Qualcomm Widevine операционной системы Android связана с копированием буфера без проверки размера входных данных. Эксплуатация уязвимости может позволить нарушителю вызвать переполнение буфера в памяти |
| Уязвимость кода | 03.01.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента Qualcomm Widevine операционной системы Android связана с копированием буфера без проверки размера входных данных. Эксплуатация уязвимости может позволить нарушителю вызвать переполнение буфера в памяти |
| Уязвимость кода | 02.01.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость загрузчика (компонент Bootloader) операционных систем Android из репозитория CAF вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать переполнение буфера на куче путем манипулирований с данными образа Qualcomm SafeSwitch |
| Уязвимость кода | 02.01.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции bta\_scan\_results\_cb\_impl (btif\_ble\_scanner.cc) операционной системы Android связана с неконтролируемым расходом ресурсов. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании при сканировании BLE (Bluetooth Low Energy) |
| Уязвимость кода | 02.01.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента MediaTek (libMtkOmxVdec.so) операционной системы Android вызвана переполнением буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код |
| Уязвимость кода | 02.01.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента Skcipher (crypto/algif\_skcipher.c) ядра операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии |
| Уязвимость кода | 02.01.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции ihevcd\_decode (ihevcd\_decode.c) операционной системы Android связана со входом в бесконечный цикл. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 02.01.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции hevcd\_parse\_slice\_header (ihevcd\_parse\_slice\_header.c) операционной системы Android связана со входом в бесконечный цикл. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании критического системного процесса |
| Уязвимость кода | 02.01.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции ihevcd\_parse\_sps (ihevcd\_parse\_headers.c) операционной системы Android связана со входом в бесконечный цикл. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании критического системного процесса |
| Уязвимость кода | 02.01.2018 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции в ihevcd\_decode.c операционной системы Android связана с утечкой памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании критического системного процесса |
| Уязвимость кода | 06.11.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции ioctl() драйвера QBT1000 в операционных системах Android для MSM, Firefox OS для MSM, QRD Android, Android из репозитория CAF связана с недостатками проверки размера буфера. Эксплуатация уязвимости может позволить нарушителю, действующему локально, вызвать переполнение буфера |
| Уязвимость кода | 06.11.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость драйвера температурного датчика Thermal Driver операционной системы Android связана с записью за границами буфера памяти и недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 06.11.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера графического процессора NVIDIA (gm20b\_clk\_throt\_set\_cdev\_state) операционной системы Linux связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса |
| Уязвимость кода | 06.11.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость драйвера MediaTek CCCI операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код в контексте привилегированного процесса |
| Уязвимость кода | 05.11.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость ядра операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии |
| Уязвимость кода | 05.11.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость компонента Media Framework операционной системы Android связана с ошибками управления ресурсом. Эксплуатация уязвимости позволяет нарушителю оказать воздействие на доступность данных |
| Уязвимость кода | 01.11.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции kgsl\_ioctl\_gpu\_command драйвера KGSL (Kernel Graphics Support Layer) ядра операционной системы Android из репозитория CAF связана с использованием памяти после её освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса с помощью специально сформированного файла |
| Уязвимость кода | 01.11.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента WLAN ядра операционной системы Android из репозитория CAF вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса с помощью специально сформированного файла |
| Уязвимость кода | 01.11.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента WLAN ядра операционной системы Android из репозитория CAF ядра операционной системы Android из репозитория CAF вызвана переполнением буфера при анализе запросов Measurement Request IE. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса с помощью специально созданного файла |
| Уязвимость кода | 01.11.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции UnpackCore ядра операционной системы Android из репозитория CAF связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса с помощью специально созданного файла |
| Уязвимость кода | 01.11.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость службы mediaanalytics компонента Media Framework операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость архитектуры | 01.11.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libmpeg2 компонента Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса с помощью специально сформированного файла |
| Уязвимость архитектуры | 01.11.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libmpeg2 компонента Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса с помощью специально сформированного файла |
| Уязвимость архитектуры | 01.11.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libavc компонента Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса с помощью специально сформированного файла |
| Уязвимость архитектуры | 01.11.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libmpeg2 компонента Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса с помощью специально сформированного файла |
| Уязвимость кода | 01.11.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость службы WindowManager компонента Framework операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 01.11.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость службы Device Policy Client (DPC) компонента Framework операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость архитектуры | 30.10.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 8,5) | Уязвимость библиотеки aac компонента Media Framework операционной системы Android связана с недостаточной проверкой состояний. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 26.10.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость библиотеки libhevc компонента Media Framework операционной системы Android связана с некорректной обработкой ошибок выделения памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 26.10.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость библиотеки libavc компонента Media Framework операционной системы Android связана с некорректной обработкой ошибок выделения памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 18.10.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции wma\_unified\_bcntx\_status\_event\_handler компонента WLAN операционной системы Android из репозитория CAF связана с чтением данных за границами буфера в памяти. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код в контексте привилегированного процесса с использованием специально сформированного файла |
| Уязвимость кода | 09.10.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость библиотеки libavc компонента Media Framework операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 27.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции wma\_send\_bcn\_buf\_ll компонента WLAN операционной системы Android из репозитория CAF связана с недостаточной проверкой вводимых данных. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код в контексте привилегированного процесса с использованием специально сформированного файла |
| Уязвимость кода | 27.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции wma\_nlo\_match\_evt\_handler компонента WLAN операционной системы Android из репозитория CAF связана с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код в контексте привилегированного процесса с использованием специально сформированного файла |
| Уязвимость кода | 26.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции wma\_p2p\_noa\_event\_handler() операционной системы Android из репозитория CAF связана с выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код в контексте привилегированного процесса с использованием специально сформированного файла |
| Уязвимость кода | 26.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции wma\_unified\_link\_peer\_stats\_event\_handler компонента WLAN операционной системы Android из репозитория CAF вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код в контексте привилегированного процесса с использованием специально сформированного файла |
| Уязвимость архитектуры | 15.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 8,5) | Уязвимость библиотеки libhevc компонента Media Framework операционной системы Android связана с недостаточной проверкой состояний. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 12.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции lim\_process\_action\_vendor\_specific компонента WLAN операционной системы Android из репозитория CAF вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, раскрыть защищаемую информацию |
| Уязвимость кода | 08.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции ih264d\_parse\_bmb\_non\_direct\_cavlc (decoder/ih264d\_parse\_bslice.c) компонента Media Framework операционной системы Android связана с ошибками управления ресурсом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, оказать воздействие на доступность данных |
| Уязвимость кода | 08.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции ih264d\_get\_implicit\_weights (decoder/ih264d\_parse\_bslice.c) компонента Media Framework операционной системы Android связана с ошибками управления ресурсами. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, оказать воздействие на доступность данных |
| Уязвимость архитектуры | 01.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libjhead службы Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость архитектуры | 01.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libgdx операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 01.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента MediaTek libmtkomxvdec операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 01.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента MediaTek teei операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 01.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента MediaTek lastbus операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 01.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость ядра MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 01.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера MediaTek Accessory Detector операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 01.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера MediaTek auxadc операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 01.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера MediaTek Accessory Detector операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость архитектуры | 01.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость неизвестной функции подсистемы памяти операционной системы Android связана с отсутствием защиты служебных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к данным ограниченного распространения |
| Уязвимость архитектуры | 01.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость средства отправки сообщений операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 01.09.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость библиотеки libhevc компонента Media Framework операционной системы Android связана с ошибками управления ресурсом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 31.08.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libhevc компонента Media Framework операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса с помощью специально сформированного файла |
| Уязвимость кода | 22.08.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость драйвера беспроводной сети операционной системы Android из репозитория CAF связана с недостаточной проверкой вводимых данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 18.08.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость во всех компонентах Qualcomm операционной системы Android из репозитория CAF, использующей ядро Linux вызвана ошибками синхронизации при использовании общего ресурса. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать состояние гонки |
| Уязвимость кода | 18.08.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость протокола передачи данных HSDPA во всех компонентах Qualcomm операционной системы Android из репозитория CAF, использующего ядро Linux, вызвана переполнением буфера. Эксплуатация уязвимости может позволить злоумышленнику, действующему удалённо, вызвать нарушение конфиденциальности, целостности и доступности защищаемой информации |
| Уязвимость кода | 15.08.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость библиотеки libstagefright компонента Media Framework операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии |
| Уязвимость кода | 14.08.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libutils операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса с помощью специально сформированного файла |
| Уязвимость архитектуры | 09.08.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 8,5) | Уязвимость библиотеки libmpeg2 компонента Media Framework операционной системы Android связана с недостаточной проверкой состояний. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость архитектуры | 09.08.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 8,5) | Уязвимость библиотеки libavc службы Media Framework операционной системы Android связана с недостаточной проверкой состояний. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 08.08.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента Bluetooth операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код в контексте привилегированного процесса с помощью специально сформированного файла |
| Уязвимость архитектуры | 03.08.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 8,5) | Уязвимость библиотеки libhevc компонента Media Framework операционной системы Android связана с недостаточной проверкой состояний. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 20.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость компонента Media Framework операционной системы Android связана с ошибками управления ресурсом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 19.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 8,5) | Уязвимость компонента Media Framework (decoder/impeg2d\_api\_main.c) операционной системы Android связана с ошибками управления ресурсом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, раскрыть защищаемую информацию |
| Уязвимость архитектуры | 19.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость загрузчика операционной системы Android из репозитория CAF связана с недостаточной проверкой размеров заголовоков разреженных загрузочных образов. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации |
| Уязвимость кода | 18.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость компонента Media Framework операционной системы Android связана с ошибками управления ресурсом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 18.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость интерфейса Audio Hardware Abstraction Layer (Hardware Abstraction Layer, HAL) компонента Media Framework операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость архитектуры | 17.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость компонента Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, раскрыть конфиденциальную информацию |
| Уязвимость кода | 14.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость компонента Camera операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 14.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента Framework (GateKeeperResponse) операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 13.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость звукового драйвера NVIDIA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код, используя локальное вредоносное приложение |
| Уязвимость кода | 13.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libmediaplayerservice службы Media Framework операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость архитектуры | 13.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libvorbis службы Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки windowmanager службы Framework операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость архитектуры | 10.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libstagefright службы Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 07.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента NVIDIA Libnvparser операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать повреждение памяти или выполнить произвольный код |
| Уязвимость архитектуры | 07.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,9) | Уязвимость в профиле персональной сети (Personal Area Networking, PAN) службы Bluetooth-стека операционной системы Android связана с неправильными требованиями уровня безопасности. Эксплуатация уязвимости позволяет нарушителю, действующему удаленно, создать сетевой интерфейс и с его помощью реализовать атаку типа «человек посередине» |
| Уязвимость кода | 07.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libminikin операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость архитектуры | 07.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость библиотеки libstagefright службы Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость пользовательского интерфейса операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость пользовательского интерфейса операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость пользовательского интерфейса операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость wi-fi драйвера Broadcom операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему локально, повысить свои привилегии |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость wi-fi драйвера Broadcom операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему локально, повысить свои привилегии |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость сетевого драйвера MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привелегии |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотек операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость звукового драйвера NVIDIA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код, используя локальное вредоносное приложение |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость звукового драйвера NVIDIA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код, используя локальное вредоносное приложение |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,9) | Уязвимость службы Bluetooth Network Encapsulation Protocol (BNEP) операционной системы Android связана с ошибками переполнения буфера в динамической памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать переполнение буфера и выполнить произвольный код на устройстве |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,9) | Уязвимость в профиле персональной сети (Personal Area Networking, PAN) службы Bluetooth Network Encapsulation Protocol (BNEP) операционной системы Android вызвана потерей разряда целого числа. Эксплуатация уязвимости позволяет нарушителю, действующему удаленно, нарушить целостность памяти и получить полный контроль над устройством |
| Уязвимость кода | 06.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функкции wma\_roam\_scan\_filter компонента WLAN операционной системы Android из репозитория CAF связана с переполнением буфера. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код в контексте привилегированного процесса с использованием специально сформированного файла |
| Уязвимость архитектуры | 04.07.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 8,5) | Уязвимость библиотеки libavc компонента Media Framework операционной системы Android связана с недостаточной проверкой состояний. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, раскрыть защищаемую информацию или вызвать отказ в обслуживании |
| Уязвимость архитектуры | 30.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента lockscreen операционной системы Android связана с ошибками в настройках безопасности. Эксплуатация уязвимости может позволить нарушителю, действующему локально, обходить блокировку PIN-кода с помощью нажатия клавиши backspace поcле каждого предложения ввести PIN |
| Уязвимость кода | 29.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента nac\_server операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему локально, повысить свои привилегии до уровня корневого пользователя |
| Уязвимость кода | 28.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента Qualcomm QTEE keymaster app операционной системы Android связана с недостаточной проверкой вводимых данных. Эксплуатация уязвимости может позволить нарушителю получить доступ к памяти |
| Уязвимость кода | 27.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 8,5) | Уязвимость компонента Media Framework (decoder/impeg2d\_dec\_hdr.c) операционной системы Android связана с ошибками управления ресурсом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, раскрыть защищаемую информацию |
| Уязвимость кода | 23.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость компонента Media Framework операционной системы Android связана с ошибками управления ресурсом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость архитектуры | 22.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libhevc службы Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость архитектуры | 21.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libstagefright компонента Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 19.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libstagefright службы Media Framework операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость архитектуры | 16.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libavc службы Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 15.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость USB-драйвера операционной системы Android из репозитория CAF вызвана ошибками синхронизации при использовании общего ресурса (состояние гонки). Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать обращение к памяти после её освобождения |
| Уязвимость кода | 15.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость видеодрайвера операционной системы Android из репозитория CAF вызвана выходом операции за границы буфера в памяти (отсутствие проверки границ в функции memcpy). Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать повреждение памяти устройства и отказ в обслуживании |
| Уязвимость кода | 15.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libeffects службы Media Framework операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 14.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента libhevc службы Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать повреждение памяти в процессе использования медиа файла и обработки данных с помощью специально созданного файла |
| Уязвимость кода | 14.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю внедрить произвольный код, используя локальное вредоносное приложение |
| Уязвимость кода | 14.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость службы Mediaserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать зависание или перезагрузку устройства с помощью специально созданного файла или отказ в обслуживании. Данная уязвимость классифицируется как уязвимость высокого уровня из-за возможности вызвать отказ в обслуживании |
| Уязвимость кода | 14.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость приложения Mediaserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании, зависание устройства и его перезагрузку при помощи специально созданного файла |
| Уязвимость кода | 14.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость приложения Mediaserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании, зависание устройства и его перезагрузку при помощи специально созданного файла |
| Уязвимость кода | 14.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость библиотеки libhevc приложения Mediaserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании, зависание устройства и его перезагрузку при помощи специально созданного файла |
| Уязвимость кода | 14.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость библиотеки libvpx приложения Mediaserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании, зависание устройства и его перезагрузку при помощи специально созданного файла |
| Уязвимость кода | 14.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера звука приложения MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 14.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость отладчика ядра FIQ операционной системы Linux связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость архитектуры | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с защитой модуля памяти eMMC от записи. Эксплуатация уязвимости может позволить злоумышленнику, действующему удалённо, нарушить конфиденциальность информации, обойдя защиту записи модуля памяти eMMC при включении питания |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость программного интерфейса PlayReady операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость криптографической программы операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения QTEE операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость программного интерфейса PlayReady операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость механизма обработки системных вызовов операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость механизма обработки системных вызовов операционной системы Android вызвана потерей разряда целого числа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции WLAN операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера ядра операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции камеры операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость загрузки файла прошивки операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера IPA операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость видео драйвера операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, реализовать «ситуацию гонки», что может вызвать модификацию общего ресурса и привести к отказу в обслуживании |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с ошибками разыменования указателей. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к локальным файлам |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента WideVine DRM операционной системы Android связана с ошибками разыменования указателей. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к локальным файлам |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость компонента Secure Display операционной системы Android вызвана ошибками синхронизации при использовании общего ресурса. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, модифицировать общий ресурс |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента Service Control Manager (SCM) операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, обойти проверку сертификата |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android вызвана целочисленным переполнением. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать другие ошибки, что может привести к отказу в обслуживании |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента WideVine DRM операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, обойти проверку сертификата |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость программного интерфейса компонента TimeZone операционной системы Android вызвана ошибками синхронизации при использовании общего ресурса. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, произвести модификацию общего ресурса |
| Уязвимость архитектуры | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость программного интерфейса компонента Hypervisor операционной системы Android связана с невыполнением аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, обойти процедуру аутентификации |
| Уязвимость архитектуры | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками контроля доступа к памяти модема. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, нарушить безопасность информации |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента WideVine DRM операционной системы Android связана с ошибками разыменования указателей. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к локальным файлам |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента WideVine DRM операционной системы Android связана с ошибками разыменования указателей. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к локальным файлам |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с ошибками проверки указателя при выполнении системных вызовов QTEE. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, обойти проверку сертификата |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость процесса RPMB операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, обойти проверку сертификата |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android вызвана наличием повышенных прав у сторонних компонентов TEEs. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера дисплея операционной системы Android связана с ошибкой повторного освобождения памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с использованием памяти после её освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к защищаемой информации |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость видеодрайвера операционной системы Android связана с использованием памяти после её освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (состояние гонки) |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость процедуры ALSA операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать повреждение стека и отказ в обслуживании |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость ioctl-обработчика драйвера звука операционной системы Android вызвана ошибками синхронизации при использовании общего ресурса. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать зависание устройства или отказ в обслуживании |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость службы обработки загрузочного образа операционной системы Android вызвана потерей разряда целого числа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать зависание и перезагрузку устройства |
| Уязвимость архитектуры | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость камеры операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, нарушить конфиденциальность информации |
| Уязвимость кода | 13.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость камеры операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к области памяти за пределами границ приложения |
| Уязвимость архитектуры | 12.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость мультимедийного фреймворка операционной системы Android связана с отсутствием защиты служебных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к защищаемым данным или выполнить произвольный код в контексте привилегированного процесса |
| Уязвимость кода | 12.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента Display операционной системы Android из репозитория CAF связана с использованием памяти после её освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса |
| Уязвимость архитектуры | 09.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libmpeg2 компонента Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в Core Kernel операционной системы Android связана с использованием памяти после её освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к защищаемой информации |
| Уязвимость архитектуры | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента TrustZone операционной системы Android связана с неправильной авторизацией. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к ресурсу |
| Уязвимость кода | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость защищенной файловой системы Secure File System (SFS) операционной системы Android вызвана целочисленным переполнением или циклическим сдвигом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к защищенной информации, управлению ресурсами или выполнению программ |
| Уязвимость кода | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в Core Kernel операционной системы Android связана с ошибками разыменования указателей. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к защищаемой информации |
| Уязвимость кода | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в загрузчике операционной системы Android связана с некорректной инициализацией ресурса. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к ресурсу |
| Уязвимость кода | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость встроенной файловой системы Embedded File System (EFS) операционной системы Android вызвана ошибками синхронизации при использовании общего ресурса. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, упростить процесс расшифровки сообщения |
| Уязвимость кода | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента WCDMA операционной системы Android связана с использованием памяти после её освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к защищаемой информации |
| Уязвимость кода | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента WCDMA операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента GERAN операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента UIM операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента GNSS операционной системы Android связана с использованием памяти после её освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к защищаемой информации |
| Уязвимость кода | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента HDR операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента 1x операционной системы Android связана с ошибками обработки чисел. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, обойти ограничения безопасности |
| Уязвимость кода | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента NAS операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость архитектуры | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в Core Kernel операционной системы Android связана с неправильной авторизацией. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к ресурсу |
| Уязвимость кода | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента TrustZone операционной системы Android связана с ошибками разыменования указателей. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к локальным файлам |
| Уязвимость кода | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента TrustZone операционной системы Android связана с непроверенным индексированием массива. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к информации |
| Уязвимость архитектуры | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость защищенной файловой системы Secure File System (SFS) операционной системы Android связана с недостатками процедуры аутентификации. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, нарушить конфиденциальность, целостность и доступность данных |
| Уязвимость кода | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента TrustZone операционной системы Android вызвана ошибками синхронизации при использовании общего ресурса. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, упростить процесс расшифровки сообщения |
| Уязвимость кода | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента TrustZone операционной системы Android связана с ошибкой повторного освобождения памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить действия, непредусмотренные интерфейсом браузера |
| Уязвимость архитектуры | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента Resource Power Manager (RPM) операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, нарушить конфиденциальность информации |
| Уязвимость кода | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента TrustZone операционной системы Android вызвана целочисленным переполнением или циклическим сдвигом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ к динамической памяти процесса или вызвать отказ в обслуживании |
| Уязвимость архитектуры | 06.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость библиотеки libhevc службы Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса |
| Уязвимость кода | 05.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера WLAN операционной системы Android из репозитория CAF вызвана ошибками синхронизации при использовании общего ресурса (состояние гонки). Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать обращение к памяти после её освобождения |
| Уязвимость архитектуры | 05.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость библиотеки libhevc службы Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 05.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента Qualcomm операционной системы Android связана с недостаточным разграничением доступа. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии и выполнить произвольный код |
| Уязвимость кода | 02.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libhevc службы Media Framework операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость архитектуры | 01.06.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libavc службы Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 30.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в медиа фреймворке (MPEG-2 decoder) операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость архитектуры | 30.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libstagefright службы Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 23.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в медиа фреймворке (libhevc) операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 22.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость в медиа фреймворке (libavc) операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 22.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость медиа платформы libstagefright операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 19.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в медиа фреймворке (H263 decoder) операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость архитектуры | 19.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в медиа фреймворке (H263 decoder) операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 18.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в мультимедийном фреймворке (AVC decoder) операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость архитектуры | 17.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libhevc службы Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 16.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость CAF-репозитория операционной системы Android вызвана ошибками синхронизации при использовании общего ресурса. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать зависание устройства (состояние гонки), используя Linux ядро |
| Уязвимость кода | 16.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libeffects службы Media Framework операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения Audioserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код при помощи локального вредоносного приложения |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость службы libstagefright приложения Mediaserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса при помощи локального вредоносного приложения |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость службы libstagefright приложения Mediaserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код при помощи локального вредоносного приложения |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции codecs/aacenc/SoftAACEncoder2.cpp службы libstagefright приложения Mediaserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса при помощи локального вредоносного приложения |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения Framework API операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и получить доступ к пользовательским разрешениям при помощи локального вредоносного приложения |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции FLACExtractor.cpp службы libstagefright приложения Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (повреждение памяти) при помощи специально созданного файла |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость службы libavc приложения Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (повреждение памяти) при помощи специально созданного файла |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость службы libhevc приложения Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (повреждение памяти) при помощи специально созданного файла |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость службы libstagefright приложения Mediaserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании, зависание устройства и перезагрузку устройства при помощи специально созданного файла |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость службы libhevc приложения Mediaserver операционной системы Android связана с ошибками управления ресурсом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании, зависание устройства и перезагрузку устройства при помощи специально созданного файла |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость подсистемы ядра trace операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера ядра Qualcomm power операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm Slimbus операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость криптодрайвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm LED операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость аудио драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость видео драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость видео драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость видео драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Wi-Fi драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость начального загрузчика Motorola операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость начального загрузчика Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость начального загрузчика Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера сенсорного экрана MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm ADSPRPC операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в libhevc приложения Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать повреждение памяти и внедрить произвольный код внутри контекста Mediaserverс помощью специально созданного файла |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в id3/ID3.cpp в libstagefright приложения Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать повреждение памяти, внедрить код внутри контекста Mediaserver с помощью специально созданного файла |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения Mediaserver в libmpeg2 операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, произвести повреждение памяти и отдаленное выполнение кода внутри контекста Mediaserver с помощью специально созданного файла |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость начального загрузчика HTC операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте загрузчика. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера сенсорного экрана Goodix операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера камеры Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm Secure Channel Manager операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера пин-контроллера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера очередности команд MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость видео драйвера MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера прерываний системного управления MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера питания MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm Secure Execution Environment Communicator операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm Secure Execution Environment Communicator операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm Secure Execution Environment Communicator операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость звукового драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость звукового драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость звукового драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость звукового драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость звукового драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость звукового драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость в HevcUtils.cpp в библиотеке libstagefright Mediaserver операционной системы Android связана с ошибками управления ресурсом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, при помощи специально сформированного файла вызвать зависание или перезагрузку устройства. Эта проблема оценивается как «низкая» из-за указанного описания уязвимости |
| Уязвимость кода | 12.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в медиа фреймворке (libmpeg2) операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 08.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в медиа фреймворке (libavc) операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 03.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента kernel/events/core.c ядра операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с наличием функций perf pmu\_register и perf\_event\_open с помощью специально созданного приложения |
| Уязвимость кода | 03.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость функции regulator\_ena\_gpio\_free компонента drivers/regulator/core.c ядра операционной системы Android связана с использованием памяти после её освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии или вызвать отказ в обслуживании (использование ресурса после его освобождения) с помощью специально созданного приложения |
| Уязвимость кода | 03.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость видеодрайвера NVIDIA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте ядра |
| Уязвимость архитектуры | 03.05.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libhevc компонента Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 25.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения для драйвера камеры операционной системы Android из репозитория CAF вызвана выходом операции за границы буфера в памяти при обработке компонента frame/command с недопустимыми значениями. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать перечитывание буфера динамической памяти |
| Уязвимость кода | 25.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость обработчика IOCTL операционной системы Android из репозитория CAF вызвана ошибками синхронизации при использовании общего ресурса (состояние гонки). Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать целочисленное переполнение и запись за границами памяти |
| Уязвимость кода | 25.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость подсистемы управления общедоступной анонимной памяти операционной системы Android из репозитория CAF связана с неправильной обработкой данных при работе с виртуальной памятью пользовательского пространства, доступной только для чтения. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать аварийный сбой в работе ядра или выполнить произвольный код при помощи специально сформированного приложения |
| Уязвимость кода | 25.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость обработчика памяти и свободных функций операционной системы Android из репозитория CAF вызвана ошибками синхронизации при использовании общего ресурса. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать использование памяти после ее освобождения |
| Уязвимость архитектуры | 24.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость библиотеки libhevc службы Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса |
| Уязвимость кода | 21.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость архитектуры | 21.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 8,3) | Уязвимость драйвера Wi-Fi операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код в контексте ядра |
| Уязвимость кода | 21.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в медиа фреймворке (libavc) операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 21.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в медиа фреймворке (libmpeg2) операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 21.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента Linux Boot операционной системы Android из репозитория CAF (Android for MSM, Firefox OS for MSM, QRD Android) связана с отсутствием проверки размера и смещения образа. Эксплуатация уязвимости может позволить нарушителю, действующему локально, вызвать целочисленное переполнение |
| Уязвимость кода | 20.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в медиа фреймворке (MPEG-2 decoder) операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 13.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость HTTP-заголовка класса URLConnection операционной системы Android существует из-за непринятия мер по нейтрализации специальных элементов. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, внедрить произвольные скрипты или установить произвольные значения в cookies |
| Уязвимость архитектуры | 13.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libstagefright службы Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера доступа Qualcomm CP операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость службы HTC OEM fastboot операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте специального процессора Sensor Hub при помощи локального вредоносного приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера сенсорного экрана Synaptics операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера сенсорного экрана Synaptics операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость видеодрайвера Qualcomm операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость звукового драйвера DTS операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте ядра операционной системы с помощью специального приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера сенсорного экрана HTC операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте ядра операционной системы с помощью специального приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость криптографического драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте ядра операционной системы с помощью специального приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Wi-Fi драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте ядра операционной системы с помощью специального приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Wi-Fi драйвера Broadcom операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте ядра операционной системы с помощью специального приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Wi-Fi драйвера Broadcom операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте ядра операционной системы с помощью специального приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Wi-Fi драйвера Broadcom операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте ядра операционной системы с помощью специального приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Wi-Fi драйвера Broadcom операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте ядра операционной системы с помощью специального приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Wi-Fi драйвера Broadcom операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте ядра операционной системы с помощью специального приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Wi-Fi драйвера Broadcom операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте ядра операционной системы с помощью специального приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Wi-Fi драйвера Broadcom операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте ядра операционной системы с помощью специального приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Wi-Fi драйвера Broadcom операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте ядра операционной системы с помощью специального приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера камеры MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте ядра операционной системы с помощью специального приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость теплового драйвера MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте ядра операционной системы с помощью специального приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость подсистемы ION операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте ядра операционной системы с помощью специального приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента SurfaceFlinger операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента Audioserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента CameraBase операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента libavc в Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код (повреждение памяти) при помощи специально сформированного медиа файла |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента libavc в Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код (повреждение памяти) при помощи специально сформированного медиа файла |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента sonivox в Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код (повреждение памяти) при помощи специально сформированного медиа файла |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента libhevc в Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код (повреждение памяти) |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента libhevc в Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код (повреждение памяти) |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента libavc в Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код (повреждение памяти) |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость компонента Qualcomm драйвера Seemp операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость аудиодрайвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера сенсорного экрана HTC операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера сенсорного экрана MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость службы libnl операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте службы Wi-Fi при помощи локального вредоносного приложения |
| Уязвимость архитектуры | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость службы libavc приложения Mediaserver операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать зависание устройства и перезагрузку устройства при помощи специально созданного файла |
| Уязвимость архитектуры | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость службы libavc приложения Mediaserver операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать зависание устройства и перезагрузку устройства при помощи специально созданного файла |
| Уязвимость архитектуры | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость службы libavc приложения Mediaserver операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать зависание устройства и перезагрузку устройства при помощи специально созданного файла |
| Уязвимость архитектуры | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость службы libavc приложения Mediaserver операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать зависание устройства и перезагрузку устройства при помощи специально созданного файла |
| Уязвимость архитектуры | 08.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость службы libskia операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать зависание устройства и перезагрузку устройства при помощи специально созданного файла |
| Уязвимость кода | 05.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера NVIDIA crypto операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 05.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера NVIDIA crypto операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 05.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера загрузки NVIDIA и процессора управления питанием операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте загрузки и процессора управления питанием. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 05.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость крипто драйвера NVIDIA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 05.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера NVIDIA I2C HID операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 04.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость подсистемы eCryptfs ядра Linux операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии при помощи большого размера стека файловой системы, который включает уровень overlayfs, связанный с fs/ecryptfs/main.c и fs/overlayfs/super.c |
| Уязвимость кода | 03.04.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость видеодрайвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код с использованием специально сформированного приложения |
| Уязвимость архитектуры | 10.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libstagefright службы Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm Wi-Fi операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, запустить приложение c привилегиями текущего пользователя |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера NVIDIA GPU операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, запустить приложение c привилегиями текущего пользователя |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера NVIDIA GPU операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера NVIDIA GPU операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, запустить приложение c привилегиями текущего пользователя |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера NVIDIA GPU операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, запустить приложение c привилегиями текущего пользователя |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера NVIDIA GPU операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, запустить приложение c привилегиями текущего пользователя |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера NVIDIA GPU операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, запустить приложение c привилегиями текущего пользователя |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость ядра подсистемы безопасности операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить код в контексте привилегированного процесса при помощи локального вредоносного приложения |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость HTC Sensor Hub Driver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость HTC Sensor Hub Driver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm IPA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Synaptics touchscreen операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Wi-Fi Qualcomm операционных систем Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость MediaTek APK операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса при помощи локального вредоносного приложения |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm camera операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm crypto engine операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm fingerprint sensor операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm fingerprint sensor операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера MediaTek hardware sensor операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm input hardware операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость ядра FIQ отладчика операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера Wi-Fi Broadcom операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость подсистемы ION ядра операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость подсистемы ION ядра операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код, а также привести к полной неработоспособности устройства и необходимости его перепрошивки |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента MediaTek, драйвера M4U, аудиодрайвера, драйвера сенсорного экрана, драйвера GPU и драйвера Command Queue операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код, а также привести к полной неработоспособности устройства и необходимости его перепрошивки |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента MediaTek, драйвера M4U, аудиодрайвера, драйвера сенсорного экрана, драйвера GPU и драйвера Command Queue операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код, а также привести к полной неработоспособности устройства и необходимости его перепрошивки |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента MediaTek, драйвера M4U, аудиодрайвера, драйвера сенсорного экрана, драйвера GPU и драйвера Command Queue операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код, а также привести к полной неработоспособности устройства и необходимости его перепрошивки |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента MediaTek, драйвера M4U, аудиодрайвера, драйвера сенсорного экрана, драйвера GPU и драйвера Command Queue операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код, а также привести к полной неработоспособности устройства и необходимости его перепрошивки |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента MediaTek, драйвера M4U, аудиодрайвера, драйвера сенсорного экрана, драйвера GPU и драйвера Command Queue операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код, а также привести к полной неработоспособности устройства и необходимости его перепрошивки |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента MediaTek, драйвера M4U, аудиодрайвера, драйвера сенсорного экрана, драйвера GPU и драйвера Command Queue операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код, а также привести к полной неработоспособности устройства и необходимости его перепрошивки |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента MediaTek, драйвера M4U, аудиодрайвера, драйвера сенсорного экрана, драйвера GPU и драйвера Command Queue операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код, а также привести к полной неработоспособности устройства и необходимости его перепрошивки |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость компонента Audioserver операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость компонента Mediaserver операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) при помощи специально сформированного файла |
| Уязвимость архитектуры | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость компонента Mediaserver операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) при помощи специально сформированного файла |
| Уязвимость архитектуры | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость компонента Mediaserver операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) при помощи специально сформированного файла |
| Уязвимость архитектуры | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость компонента Mediaserver операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) при помощи специально сформированного файла |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость компонента Mediaserver операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) при помощи специально сформированного файла |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость компонента Mediaserver операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) при помощи специально сформированного файла |
| Уязвимость архитектуры | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость компонента Mediaserver операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) при помощи специально сформированного файла |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения NFC операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса. Эта проблема оценивается как «высокая», потому что она может быть использована для получения локального доступа к повышенным возможностям, которые в обычном режиме недоступны сторонним приложениям |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения Audioserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте привилегированного процесса. Эта проблема оценивается как «высокая», потому что она может быть использована для получения локального доступа к повышенным возможностям, которые в обычном режиме недоступны сторонним приложениям |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения Audioserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте привилегированного процесса. Эта проблема оценивается как «высокая», потому что она может быть использована для получения локального доступа к повышенным возможностям, которые в обычном режиме недоступны сторонним приложениям |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость верификатора восстановления операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «критически важная» из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать повреждение памяти во время обработки медиа файлов и данных с помощью специально сформированного файла. Эта проблема оценивается как «критически важная» из-за возможности удаленного выполнения кода в контексте работы Mediaserver |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать повреждение памяти во время обработки медиа файлов и данных с помощью специально сформированного файла. Эта проблема оценивается как «критически важная» из-за возможности удаленного выполнения кода в контексте работы Mediaserver |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать повреждение памяти во время обработки медиа файлов и данных с помощью специально сформированного файла. Эта проблема оценивается как «критически важная» из-за возможности удаленного выполнения кода в контексте работы Mediaserver |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать повреждение памяти во время обработки медиа файлов и данных с помощью специально сформированного файла. Эта проблема оценивается как «критически важная» из-за возможности удаленного выполнения кода в контексте работы Mediaserver |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать повреждение памяти во время обработки медиа файлов и данных с помощью специально сформированного файла. Эта проблема оценивается как «критически важная» из-за возможности удаленного выполнения кода в контексте работы Mediaserver |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать повреждение памяти во время обработки медиа файлов и данных с помощью специально сформированного файла. Эта проблема оценивается как «критически важная» из-за возможности удаленного выполнения кода в контексте работы Mediaserver |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать повреждение памяти во время обработки медиа файлов и данных с помощью специально сформированного файла. Эта проблема оценивается как «критически важная» из-за возможности удаленного выполнения кода в контексте работы Mediaserver |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать повреждение памяти во время обработки медиа файлов и данных с помощью специально сформированного файла. Эта проблема оценивается как «критически важная» из-за возможности удаленного выполнения кода в контексте работы Mediaserver |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать повреждение памяти во время обработки медиа файлов и данных с помощью специально сформированного файла. Эта проблема оценивается как «критически важная» из-за возможности удаленного выполнения кода в контексте работы Mediaserver |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Wi-Fi драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость сетевого драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость сетевого драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера камеры Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm ADSPRPC операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm IPA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость архитектуры | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость загрузчика Qualcomm операционной системы Android связана с отсутствием защиты служебных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте загрузчика. Эта проблема оценивается как «высокая», потому что представляет собой общий обход углубленного уровня защиты загрузчика или использование технологии снижения последствий воздействий |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера Qualcomm GPU операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 08.03.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm GPU операционной системы Android связана с недостатками разграничения доступа (необходимо получить доступ к привилегированному процессу и изменить текущую конфигурацию платформы). Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 15.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость звукового драйвера мобильного приложения MSM для операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать целочисленное переполнение, за которым следует переполнение буфера, в случае, если название функции имеет большую длину |
| Уязвимость архитектуры | 14.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость библиотеки libstagefright службы Media Framework операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента Audioserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Broadcom Wi-Fi операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера HTC touchscreen операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера HTC touchscreen операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера HTC touchscreen операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Realtek sound операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера звука Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm Secure Execution Environment Communicator операционной системы Linux связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Wi-Fi Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Wi-Fi Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Wi-Fi Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Wi-Fi Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код в контексте ядра при помощи локального вредоносного приложения |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Qualcomm Wi-Fi драйвера операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Qualcomm Wi-Fi драйвера операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Qualcomm Wi-Fi драйвера операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Qualcomm Wi-Fi драйвера операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Qualcomm Wi-Fi драйвера операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Qualcomm Wi-Fi драйвера операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Qualcomm Wi-Fi драйвера операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость звукового драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость звукового драйвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера сенсорного экрана Synaptics операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте чипсета сенсорного экрана. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера сенсорного экрана Synaptics операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте чипсета сенсорного экрана. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость Broadcom Wi-Fi драйвера операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «критическая» из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость NVIDIA GPU драйвера операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «критическая» из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость NVIDIA GPU драйвера операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «критическая» из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера файловой системы ядра операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить локальному вредоносному приложению произвольный код в контексте ядра. Эта проблема оценивается как «критическая» из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость Bionic DNS операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать зависание или перезагрузку устройства. Эта проблема оценивается как «высокая» из-за возможности удаленного вызова отказа в обслуживании |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в Audioserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса. Эта проблема оценивается как «высокая», потому что она может быть использована для получения доступа к возможностям более высокого уровня, которые в обычном режиме недоступны сторонним приложениям |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в Audioserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса. Эта проблема оценивается как «высокая», потому что она может быть использована для получения доступа к возможностям более высокого уровня, которые в обычном режиме недоступны сторонним приложениям |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в Audioserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса. Эта проблема оценивается как «высокая», потому что она может быть использована для получения доступа к возможностям более высокого уровня, которые в обычном режиме недоступны сторонним приложениям |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в Audioserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса. Эта проблема оценивается как «высокая», потому что она может быть использована для получения доступа к возможностям более высокого уровня, которые в обычном режиме недоступны сторонним приложениям |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в Mediaserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте привилегированного процесса. Эта проблема оценивается как «высокая», потому что она может быть использована для получения доступа к возможностям более высокого уровня, которые в обычном режиме недоступны сторонним приложениям |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость службы Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, внедрить произвольный код, используя специально созданный файл, что может вызвать повреждение памяти во время чтения медиа файла или других данных. Данная уязвимость расценивается как критическая из-за возможности внедрения произвольного кода внутри контекста службы Mediaserver, что оказывает влияние на библиотеку libhevc |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость службы Mediaserver операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, внедрить произвольный код, используя специально созданный файл, что может вызвать повреждение памяти во время чтения медиа файла или других данных. Данная уязвимость расценивается как критическая из-за возможности внедрения произвольного кода внутри контекста службы Mediaserver, что оказывает влияние на библиотеку libhevc |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость службы Surfaceflinger операционной системы Android вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, внедрить произвольный код с помощью специально созданного файла, что может вызвать повреждение памяти во время чтения медиа файла или других данных. Данная уязвимость расценивается как критическая из-за возможности внедрения произвольного кода внутри контекста службы Surfaceflinger |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость программного интерфейса Framework операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, внедрить произвольный код, используя локальное вредоносное приложение |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость программного интерфейса Framework операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, внедрить произвольный код, используя локальное вредоносное приложение |
| Уязвимость кода | 08.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость программного интерфейса Framework операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, внедрить произвольный код с помощью локального вредоносного приложения |
| Уязвимость кода | 07.02.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции aio\_mount в fs/aio.c ядра Linux операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему локально, из-за неправильного ограничения доступа к выполнению, обойти политику ограничений SELinux W^X и повысить свои привилегии при помощи системного вызова io\_setup |
| Уязвимость кода | 18.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Broadcom Wi-Fi операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 18.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера Broadcom Wi-Fi операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 13.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции camera\_fdvt.c драйвера MT6573FDVT\_SetRegHW приложения MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость превышения привилегий в видеодрайвере Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как критичная из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость превышения привилегий в драйвере NVIDIA GPU операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как критичная из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость превышения привилегий в драйвере Qualcomm GPU операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как критичная из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость превышения привилегий в драйвере NVIDIA GPU операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как критичная из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость превышения привилегий в драйвере NVIDIA GPU операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как критичная из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость превышения привилегий в драйвере NVIDIA GPU операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как критичная из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость превышения привилегий в драйвере NVIDIA GPU операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как критичная из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость превышения привилегий в драйвере NVIDIA GPU операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как критичная из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость превышения привилегий в драйвере NVIDIA GPU операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как критичная из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера Broadcom Wi-Fi ядра операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код через вредоносное приложение |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Broadcom Wi-Fi ядра операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код через вредоносное приложение |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Broadcom Wi-Fi ядра операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код через вредоносное приложение |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm Wi-Fi ядра операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код через вредоносное приложение |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm sound ядра операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код через вредоносное приложение |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера NVIDIA GPU ядра операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код через вредоносное приложение |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm camera ядра операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код через вредоносное приложение |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость конфигурации подсистем Page Table операционной системы Android вызвана ошибками в процедуре авторизации. Эксплуатация уязвимости может позволить нарушителю, действующему локально, получить несанкционированный доступ к памяти гипервизора |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость гипервизора операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему локально, получить несанкционированный доступ к памяти гипервизора при помощи HLOS |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость гипервизора операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему локально, вызвать отказ в обслуживании через специально сформированное имя директории, задаваемое в параметре uid, связанном с именем WAR-файла, содержащегося в том числе в POST-запросе |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость конфигурации приложения Binder операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Broadcom Wi-Fi операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Broadcom Wi-Fi операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Broadcom Wi-Fi операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера сенсора Synaptics операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Broadcom Wi-Fi операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Broadcom Wi-Fi операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента Wi-Fi операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость службы Mediaserver операционной системы Android связана с ошибками управления ресурсом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, привести к зависанию или перезагрузке устройства |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Множественные уязвимости libmedia и libstagefright медиа-сервера операционной системы Android связана с неправильной обработкой данных. Эксплуатация уязвимостей может позволить нарушителю, действующему удалённо, вызвать зависание или перезагрузку устройства |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость libstagefright медиа-сервера операционной системы Android связана с неправильной обработкой данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, привести к зависанию или перезагрузке устройства |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость службы медиа-сервера операционной системы Android связана с ошибками управления ресурсом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, привести к зависанию или перезагрузке устройства |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость службы Telephony операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать зависание или перезагрузку устройства |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость медиа-кодеков Qualcomm операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость медиа-кодеков Qualcomm операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость медиа-кодеков Qualcomm операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость медиа-кодеков Qualcomm операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость превышения привилегий в библиотеке NVIDIA libomx (libnvomx) операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте привилегированного процесса. Эта проблема оценивается как «высокая», потому что она может быть использована, чтобы получить локальный доступ к расширенным возможностям, которые обычно недоступны сторонним приложениям |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость превышения привилегий в библиотеке NVIDIA libomx (libnvomx) операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте привилегированного процесса. Эта проблема оценивается как «высокая», потому что она может быть использована, чтобы получить локальный доступ к расширенным возможностям, которые обычно недоступны сторонним приложениям |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость превышения привилегий драйвера MediaTek I2C операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость превышения привилегий драйвера MediaTek операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость превышения привилегий драйвера MediaTek операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость превышения привилегий драйвера MediaTek операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость превышения привилегий драйвера MediaTek операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость превышения привилегий драйвера аудио кодека HTC операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость превышения привилегий драйвера аудио кодека HTC операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость превышения привилегий драйвера аудио кодека HTC операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость превышения привилегий в драйвере NVIDIA GPU операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «критичная» из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость превышения привилегий в драйвере NVIDIA GPU операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «критичная» из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость превышения привилегий в драйвере NVIDIA GPU операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «критичная» из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость компонента Telephony операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость службы libvpx медиасервера операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить злоумышленнику, действующему удалённо, нарушить конфиденциальность информации |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость функции VBRISeeker.cpp службы libstagefright медиасервера операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить злоумышленнику, действующему удалённо, нарушить конфиденциальность информации |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость функции decoder/ihevcd\_decode.c службы libhevc медиасервера операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить злоумышленнику, действующему удалённо, нарушить конфиденциальность информации |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость функции Tremolo/dpen.s медиасервера операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить злоумышленнику, действующему удалённо, нарушить конфиденциальность информации |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость службы базовой сети операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить злоумышленнику, действующему удалённо, обойти проверку сертификата |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость медиасервера операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libnl операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость аудиосервера операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции lvm/wrapper/Bundle/EffectBundle.cpp службы libeffects аудиосервера операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость Framework API операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции silk/NLSF\_stabilize.c службы libopus медиасервера операционной системы Android вызвана выходом операции за границы буфера на стеке. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить несанкционированный доступ к устройству при помощи специально сформированного файла |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость файловой системы Qualcomm FUSE операционной системы Android связана с ошибками управления ресурсом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, использовать специально сконструированный файл, чтобы вызвать зависание или перезагрузку устройства. Эта проблема оценивается как «высокая» из-за возможности удаленного вызова отказа в обслуживании |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера сенсорного экрана Synaptics операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость компонент MediaTek, включая драйвер контроля температуры и видео драйвер, операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость компонент MediaTek, включая драйвер контроля температуры и видео драйвер, операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость компонент MediaTek, включая драйвер контроля температуры и видео драйвер, операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость компонент MediaTek, включая драйвер контроля температуры и видео драйвер, операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «критичная» из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в начальном загрузчике Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «критичная» из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в начальном загрузчике Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «критичная» из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость подсистемы управления звуком операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость подсистемы управления производительностью ядра операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера NVIDIA GPU операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «критичная» из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера NVIDIA GPU операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «критичная» из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера NVIDIA GPU операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «критичная» из-за возможности компрометации локального устройства, которое может потребовать перепрошивки операционной системы для восстановления устройства |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость Wi-Fi драйвера Qualcomm операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость камеры Qualcomm операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость ядра сетевой подсистемы операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «умеренная», потому что сначала требует компрометации привилегированного процесса и оптимизации текущего компилятора для ограничения доступа к уязвимому коду |
| Уязвимость кода | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость в драйвере камеры NVIDIA операционной системы Android связана с ошибками в коде. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызывать локально постоянный отказ в обслуживании, который может потребовать перепрошивки операционной системы для восстановления устройства. Эта проблема оценивается как «высокая» из-за возможности вызвать локально постоянный отказ в обслуживании |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера сенсорного экрана Synaptics операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера сенсорного экрана Synaptics операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость в звуковом драйвере Qualcomm операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость в звуковом драйвере Qualcomm операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость в звуковом драйвере Qualcomm операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера MediaTek операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость архитектуры | 12.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость в драйвере камеры Qualcomm операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код локального вредоносного приложения в контексте ядра. Эта проблема оценивается как «высокая», потому что сначала требует компрометации привилегированного процесса |
| Уязвимость кода | 04.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции аудио драйвера мобильного приложения MSM для операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать целочисленное переполнение, за которым следует переполнение буфера, если установлены большие значения некоторых переменных в пространстве пользователя. В другой функции отсутствие проверки нижней границы может привести к доступу за границами памяти |
| Уязвимость кода | 03.01.2017 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 8,3) | Уязвимость драйвера для видеокарты мобильного приложения MSM для операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать переполнение динамической области памяти из-за использования для вычисления смещений и размеров для операции копирования переменной, управляемой из пространства пользователя |
| Уязвимость кода | 29.12.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента Qualcomm Sound Codec операционной системы Android связана с недостаточным разграничением доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии и выполнить произвольный код с использованием специально сформированного приложения |
| Уязвимость кода | 28.12.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость аудио драйвера мобильного приложения MSM для операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать целочисленное переполнение, за которым следует переполнение динамической области памяти буфера, в случае, если название функции имеет большую длину |
| Уязвимость кода | 27.12.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость аудио драйвера операционной системы Android CAF-сборки связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, в случае, если проверка работоспособности выявила значение длины в неправильном диапазоне и выведено сообщение об ошибке, продолжить выполнение кода таким же образом, как и для правильного значения длины |
| Уязвимость кода | 22.12.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в обработчике функции ioctl мобильного приложения MSM для операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить доступ за границами памяти из-за отсутствия нескольких проверок работоспособности |
| Уязвимость кода | 22.12.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость мобильного приложения MSM для операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать перезагрузку устройства после сбоя работы ядра из-за того, что когда управляющий объект, связанный с кодеком, передается из пространства пользователя, преобразование типов выполняется в структуру хранения вместо структуры самого кодека |
| Уязвимость кода | 10.12.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость аудио драйвера мобильного приложения MSM для операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выбрать значения некоторых переменных в пространстве пользователя, которые могут вызвать переполнение стека |
| Уязвимость архитектуры | 06.12.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость компонента GPS операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (приостановку обнаружения сигнала GPS), используя некорректный файл xtra.bin или xtra2.bin на фальсификационном хосте Qualcomm gpsonextra.net или хосте izatcloud.net |
| Уязвимость кода | 29.11.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость начального загрузчика устройств Motorola операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 29.11.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость начального загрузчика устройств Huawei операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 29.11.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера SoC-микросхем MediaTek операционной системы Android. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 29.11.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость начального загрузчика устройств HTC операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 29.11.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость Wi-Fi драйвера Broadcom операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии |
| Уязвимость кода | 15.11.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера камеры операционной системы Android из репозитория CAF связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, осуществить перезапись в памяти ядра |
| Уязвимость кода | 13.10.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость загрузчика операционной системы Android из репозитория CAF вызвана целочисленным переполнением. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код в контексте ядра |
| Уязвимость кода | 06.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость стека IPv6 ядра Linux операционной системы Android связана с использованием памяти после её освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему локально, повысить свои привилегии или вызвать отказ в обслуживании (аварийное завершение работы) с помощью специально созданного системного вызова |
| Уязвимость кода | 06.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость файла drivers/media/platform/msm/camera\_v2/pproc/cpp/msm\_cpp.c компонента Qualcomm операционной системы Android связана с отсутствием проверки состояния потока. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 06.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость файла drivers/media/platform/msm/camera\_v2/isp/msm\_isp\_axi\_util.c компонента Qualcomm операционной системы Android связана с тем, что проверка индексов массива осуществляется не должным образом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 06.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость файла sound/soc/msm/qdsp6v2/q6lsm.c компонента Qualcomm операционной системы Android вызвана целочисленным переполнением. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 06.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость файла drivers/video/msm/mdp4\_util.c компонента Qualcomm операционной системы Android связана с отсутствием проверки назначения переменных num\_r\_stages, num\_g\_stages, num\_b\_stages. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 06.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера камеры MSM компонента Qualcomm операционной системы Android связана с отсутствием проверки входящих параметров. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 06.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость файла drivers/misc/qseecom.c компонентов Qualcomm операционной системы Android связана с отсутствием проверки некоторых адресов буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения, позволяющего сделать вызов ioctl |
| Уязвимость кода | 06.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость файла drivers/media/platform/msm/camera\_v2/sensor/cci/msm\_cci.c компонентов Qualcomm операционной системы Android связана с ошибкой неучтенной единицы. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения, которое посылает команду l2C |
| Уязвимость кода | 06.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость файла drivers/misc/qseecom.c компонентов Qualcomm операционной системы Android связана с отсутствием проверки длины данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 06.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость файла drivers/media/platform/msm/camera\_v2/isp/msm\_isp\_util.c компонентов Qualcomm операционной системы Android вызвана множественным переполнением буфера. Эксплуатация уязвимостей может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 06.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость ядра Linux версии до 3.11 на ARM платформах операционной системы Android связана с неправильным рассмотрением доступа пользовательского пространства к регистру TPIDRURW. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 06.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость файла drivers/media/platform/msm/camera\_v2/isp/msm\_isp\_stats\_util.c компонентов Qualcomm операционной системы Android связана с отсутствием проверки некоторых значений индексов. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 06.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость файла drivers/media/platform/msm/camera\_v2/isp/msm\_isp\_axi\_util.c компонентов Qualcomm операционной системы Android связана с отсутствием проверки количества потоков. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 06.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость файла drivers/media/platform/msm/camera\_v2/sensor/csid/msm\_csid.c компонентов Qualcomm операционной системы Android связана с отсутствием проверки некоторых параметров. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость архитектуры | 06.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость файла drivers/misc/qseecom.c компонентов Qualcomm операционной системы Android связана с неправильным ограничением ввода пользовательского пространства. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 06.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость файла drivers/misc/qseecom.c компонентов Qualcomm операционной системы Android связана с отсутствием проверки вызовов ioctl. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 06.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера diag компонентов Qualcomm операционной системы Android вызвана потерей разряда целого числа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии или получить конфиденциальную информацию с помощью специально созданного приложения |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость ядра операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость начального загрузчика LG Electronics операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии за счет использования доступа к привилегированному процессу |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера NVIDIA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Serial Peripheral Interface операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость медиа-сервера операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с тем, что должным образом не ограничивается выполнение кода в контексте ядра. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера Qualcomm GPU операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента Shell операционной системы Android связана с тем, что управление правами доступа MANAGE\_USERS и CREATE\_USERS осуществляется не должным образом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, обойти существующие ограничения доступа с помощью специально созданного приложения |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 8,3) | Уязвимость фреймворка API операционной системы Android связана с отсутствием гарантий того, что данные пакета возникли из системы управления пакетами. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, обойти механизмы защиты с помощью специально созданного приложения |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость метода codecs/aacdec/SoftAAC2.cpp библиотеки libstagefright медиа-сервера операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) с помощью специально сформированных данных ADTS |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость декодера ih264d медиа-сервера операционной системы Android связана с тем, что не инициализируются некоторые части структуры. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) при помощи специально сформированного медиа файла |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость файла decoder/ih264d\_api.c медиа-сервера операционной системы Android связана с неправильным управлением недопустимыми блоками PPS и SPS. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) при помощи специально сформированного медиа файла |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость метода codecs/hevcdec/SoftHEVC.cpp библиотеки libstagefright медиа-сервера операционной системы Android связана с неправильным управлением ошибками декодера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) при помощи специально сформированного медиа файла |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость файла exif.c инструмента jhead 2.87, который используется в библиотеке libjhead операционной системы Android, вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код или вызвать отказ в обслуживании с помощью специально сформированных данных EXIF |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость файла services/core/java/com/android/server/pm/PackageManagerService.java фреймворка API операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить приоритет фильтра intent-filter с помощью специально созданного приложения |
| Уязвимость архитектуры | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость Wi-Fi драйвера компонента Qualcomm операционной системы Android связана с неправильными вызовами функции snprintf. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) с помощью специально сформированных фреймов |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость видеодрайвера в ядре операционной системы Android. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость пакета libmedia медиасервера операционной системы Android связана с ошибками разыменования указателей. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код или вызвать отказ в обслуживании (разыменование нулевого указателя, повреждение памяти) при помощи специально сформированного медиа файла |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость декодера ih264d медиасервера операционной системы Android связана с неправильной обработкой номеров фрагментов. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) при помощи специально сформированного медиа файла |
| Уязвимость кода | 05.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость файла codecs/on2/h264dec/source/h264bsd\_dpb.c библиотеки libstagefright медиасервера операционной системы Android вызвана целочисленным переполнением. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) при помощи специально сформированного медиа файла |
| Уязвимость кода | 01.08.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость службы ServiceManager (cmds/servicemanager/service\_manager.c) операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость архитектуры | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость библиотеки libc операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) с помощью специально сформированного файла |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость ядра видео-драйвера операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера шины SPI операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера шины SPI операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера дисплея MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера управления питанием операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера управления питанием операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость реализации ядра операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость реализации ядра файловой системы операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость GPS драйвера MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость видео драйвера MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость видео драйвера MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера аппаратного сенсора MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость Wi-Fi драйвера Qualcomm операционной системы Android связана с ошибками в коде. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера питания MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера питания MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера камеры NVIDIA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость файла CORE/HDD/src/wlan\_hdd\_hostapd.c Wi-Fi драйвера Qualcomm операционной системы Android связана с ошибками процедуры копирования данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость реализации файловой системы ядра операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость видео драйвера NVIDIA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость модуля производительности Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость Wi-Fi драйвера MediaTek операционной системы Android связана с ошибками управления ресурсом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость файла MPEG4Extractor.cpp компонента libstagefright медиасервера операционной системы Android связана с отсутствием процедуры проверки выделения памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) с помощью специально сформированного файла |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость подсистемы сокетов операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения, использующего сокет AF\_MSM\_IPC или любой другой, не объявленный в SELinux |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Множественные уязвимости файла libdex/OptInvocation.cpp компонента DexClassLoader операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимостей может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения, работающего с длинными именами файлов |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость файла Tremolo/res012.c медиасервера операционной системы Android связана с отсутствием проверки номеров разделов. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) при помощи специально сформированного медиа файла |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость файла decoder/ih264d\_parse\_pslice.c медиасервера операционной системы Android связана с ошибками обработки кадров. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) при помощи специально сформированного медиа файла |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость медиасервера операционной системы Android связана с отсутствием ограничений на использование памяти процессом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) при помощи специально сформированного медиа файла |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость скрипта internal/app/ChooserActivity.java службы ChooserTarget операционной системы Android связана с ошибками в обработке меток безопасности. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость библиотеки libpng операционной системы Android связана с ошибками в коде. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость файла libs/binder/Parcel.cpp программного интерфейса фреймворка Parcels операционной системы Android связана с отсутствием проверки возвращаемого значения системного вызова. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, обойти защитный механизм изолированной среды выполнения программ с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость подсистемы сокетов операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, обойти существующие ограничения системных вызовов с помощью специально созданного приложения, создающего вызов ioctl |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость компонента mm-video-v4l2 vdec операционной системы Android связана с использованием памяти после её освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Множественные уязвимости медиасервера операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимостей может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость файла decoder/ih264d\_api.c медиасервера операционной системы Android связана с ошибками инициализации структур данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) при помощи специально сформированного медиа файла |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость файла decoder/ih264d\_process\_intra\_mb.c медиасервера операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) при помощи специально сформированного медиа файла |
| Уязвимость кода | 11.07.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Уязвимость декодера H.264 медиасервера операционной системы Android связана с ошибками инициализации данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) при помощи специально сформированного медиа файла |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента libstagefright медиасервера операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость файла mp3dec/SoftMP3.cpp компонента libstagefright медиасервера операционной системы Android связана с отсутствием дополнительной проверки соотношения размеров выделенной памяти и размеров кадра. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента libstagefright медиасервера операционной системы Android связана с отсутствием проверки размера OMX буфера для кодеков GSM и G711. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента libstagefright медиасервера операционной системы Android связана с отсутствием проверки размера OMX буфера для кодеков GSM и G711. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента mm-video-v4l2 venc медиасервера операционной системы Android связана с неправильной обработкой размера буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента mm-video-v4l2 venc медиасервера операционной системы Android связана с неправильной обработкой размера буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента mm-video-v4l2 venc медиасервера операционной системы Android связана с неправильной обработкой размера буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента mm-video-v4l2 vidc медиасервера операционной системы Android связана с отсутствием проверки структур данных OMX параметра. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонентаmm-video-v4l2 vdec медиасервера операционной системы Android связана с неправильной обработкой размера буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость файла mm-video-v4l2/vidc/vdec/src/omx\_vdec\_msm8974.cpp медиасервера операционной системы Android связана с неправильной обработкой указателей. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость файла mm-video-v4l2/vidc/vdec/src/omx\_vdec\_msm8974.cpp медиасервера операционной системы Android связана с неправильной обработкой указателей. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость медиасервера операционной системы Android связана с отсутствием проверки размера OMX буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость функции в SampleTable.cpp библиотеки libstagefright компонента mediaserver операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (зависание и перезагрузка устройства) с помощью специально сформированного файла |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции в sdcard/sdcard.c операционной системы Android связана с нарушением граничных условий в алгоритме. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера Broadcom Wi-Fi операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера управления питанием MediaTek операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера камеры NVIDIA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера камеры NVIDIA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость видеодрайвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость видеодрайвера Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость Wi-Fi драйвера Qualcomm операционной системы Android связана с ошибками в коде. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость Wi-Fi драйвера Qualcomm операционной системы Android связана с ошибками в коде. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость Wi-Fi драйвера Qualcomm операционной системы Android связана с ошибками в коде. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость Wi-Fi драйвера Qualcomm операционной системы Android связана с ошибками в коде. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость Wi-Fi драйвера Qualcomm операционной системы Android связана с ошибками в коде. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость звукового драйвера Qualcomm операционной системы Android связана с ошибками в коде. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера Qualcomm GPU операционной системы Android связана с ошибками в коде. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость звукового драйвера Qualcomm операционной системы Android связана с ошибками в коде. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость аудио драйвера Qualcomm операционной системы Android связана с ошибками в коде. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость видеодрайвера Qualcomm операционной системы Android связана с ошибками в коде. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libvpx в libwebm компонента mediaserver операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) при помощи специально созданного mkv-файла |
| Уязвимость кода | 13.06.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,5) | Множественные уязвимости в h264dec библиотеки libstagefright компонента mediaserver операционной системы Android вызваны целочисленным переполнением. Эксплуатация уязвимостей может позволить нарушителю, действующему удалённо, выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) при помощи специально сформированного медиа файла |
| Уязвимость кода | 17.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость реализации модуля adb операционной системы Android связана с некорректной обработкой операции закрытия сокета. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость кодека Qualcomm hardware video codec операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (перезагрузку устройства) с помощью специального сформированного файла |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость медиадрайвера NVIDIA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость медиадрайвера NVIDIA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость медиадрайвера NVIDIA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость драйвера Qualcomm MDP операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера Qualcomm buspm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера Qualcomm buspm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость видеодрайвера NVIDIA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость видеодрайвера NVIDIA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость видеодрайвера NVIDIA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость видеодрайвера NVIDIA операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента Qualcomm TrustZone операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента Qualcomm TrustZone операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость функции OpenSSLCipher.java компонента Conscrypt операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, подменить аутентификационное сообщение |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость функции OpenSSLCipher.java компонента Conscrypt операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, подменить аутентификационное сообщение |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции codecs/amrnb/dec/SoftAMR.cpp, используемой в libstagefright компонента mediaserver операционной системы Android, существует из-за отсутствия проверки размера буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции codecs/on2/dec/SoftVPX.cpp в libstagefright компонента mediaserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции codecs/on2/enc/SoftVPXEncoder.cpp в libstagefright компонента mediaserver операционной системы Android связана с отсутствием проверки размера OMX-буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции services/camera/libcameraservice/device3/Camera3Device.cpp компонента mediaserver операционной системы Android существует из-за отсутствия проверки идентификаторов шаблонов. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции media/libmediaplayerservice/nuplayer/NuPlayerStreamListener.cpp компонента mediaserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции libs/binder/IPCThreadState.cpp компонента Binder операционной системы Android существует из-за некорректных ссылок на объекты. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции libbacktrace/Backtrace.cpp компонента debuggerd операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии при помощи приложения, содержащего специально созданное символьное имя |
| Уязвимость кода | 09.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость в файле server/TetherController.cpp операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, обойти существующие ограничения доступа с помощью специально созданного приложения |
| Уязвимость кода | 06.05.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость во всех компонентах Qualcomm операционной системы Android из репозитория CAF, использующей ядро Linux, вызвана выходом операции за границы буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании |
| Уязвимость кода | 18.04.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции rootdir/init.rc операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость архитектуры | 18.04.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость функции exchange/eas/EasAutoDiscover.java в реализации Autodiscover компонента Exchange ActiveSync операционной системы Android связана с отсутствием защиты служебных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить конфиденциальную информацию с помощью специально созданного приложения, которое запускает поддельный ответ на запрос Get |
| Уязвимость кода | 18.04.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции media/libmedia/IOMX.cpp компонента mediaserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 18.04.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции include/core/SkPostConfig.h графической библиотеки Skia компонента System\_server операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии (аварийное завершение работы) с помощью специально созданного приложения |
| Уязвимость кода | 18.04.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера ядра Qualcomm Power Management операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения, использующего корневой доступ |
| Уязвимость кода | 18.04.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера ядра компонента Texas Instruments операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 18.04.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Множественные уязвимости функции minzip/SysUtil.c компонента Recovery Procedure операционной системы Android вызваны целочисленным переполнением. Эксплуатация уязвимостей может позволить нарушителю, действующему локально, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 18.04.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента Download Manager операционной системы Android существует из-за недостаточной проверки состояния ресурса при возможности его совместного использования. Эксплуатация уязвимости может позволить нарушителю, действующему локально, обойти существующие ограничения доступа к частным файлам с помощью специально созданного приложения, которое меняет ссылку |
| Уязвимость кода | 18.04.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента Telecom Component операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему локально, подменить при вызове номер телефона с помощью специально созданного приложения |
| Уязвимость кода | 18.04.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции libs/binder/IMemory.cpp компонента IMemory Native Interface операционной системы Android существует из-за неправильного расчёта размера кучи. Эксплуатация уязвимости может позволить нарушителю, действующему локально, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 18.04.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость драйвера Qualcomm RF операционной системы Android вызвана некорректным ограничением доступа к ioctl-вызовам сокета. Эксплуатация уязвимости может позволить нарушителю, действующему локально, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 18.04.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента Qualcomm ARM операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему локально, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 18.04.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость функции в server/content/SyncStorageEngine.java компонента SyncStorageEngine операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании с помощью специально созданного приложения |
| Уязвимость кода | 18.04.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента Wi-Fi операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.03.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Множественные уязвимости библиотеки libeffects in mediaserver операционной системы Android вызваны целочисленным переполнением. Эксплуатация уязвимостей может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.03.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libcameraservice компонента mediaserver операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.03.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,6) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения, которое использует доступ conn\_launcher |
| Уязвимость кода | 13.03.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость ядра драйвера MediaTek Wi-Fi операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 13.03.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента Qualcomm операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 07.02.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 8,3) | Уязвимость Wi-Fi драйвера Broadcom операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) при помощи специальным образом сформированных пакетов сообщений |
| Уязвимость кода | 07.02.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость функции get\_build\_id файла elf\_utils.cpp приложения Debuggerd операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему локально, повысить свои привилегии с помощью специально созданного приложения, которое некорректно обрабатывает элемент Desk Size в ELF файлах |
| Уязвимость кода | 07.02.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость драйвера Qualcomm Wi-Fi ядра операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему локально, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 07.02.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость модуля производительности процессоров Qualcomm ARM операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему локально, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 07.02.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость функции BnCrypto::onTransact function (media/libmedia/ICrypto.cpp) операционной системы Android вызвана целочисленным переполнением. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, обойти механизмы защиты и получить конфиденциальную информацию, вызвав расчёты некорректного размера |
| Уязвимость кода | 07.02.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 8,3) | Уязвимость функции wifi\_cleanup function (bcmdhd/wifi\_hal/wifi\_hal.cpp) компонента Wi-Fi операционной системы Android связана с использованием памяти после её освобождения. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии за счёт получения доступа к локальной физической среде во время выполнения специально созданного приложения |
| Уязвимость кода | 07.02.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость операционной системы Android связана с недостатками разграничения доступа при аутентификации пользователя. Эксплуатация уязвимости может позволить нарушителю, действующему локально, использовать среду Trusted Execution Environment (TEE) без проверки подлинности и воспроизводить ранее перехваченные ответы за счет слабозащищенных криптографических маркеров аутентификации (AuthTokens) |
| Уязвимость кода | 06.01.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения Widevine QSEE TrustZone операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения, использующего QSEECOM |
| Уязвимость кода | 06.01.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость реализации System V IPC ядра операционной системы Android связана с ошибками управления ресурсом. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (исчерпание ресурсов ядра) путём использования недостатков межпроцессного взаимодействия и управления памятью |
| Уязвимость кода | 06.01.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость приложения операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (длительную перезагрузку) с помощью специально созданного приложения |
| Уязвимость кода | 06.01.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость мастера настройки операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему локально, изменить настройки или обойти механизм защиты от сброса к заводским настройкам |
| Уязвимость кода | 06.01.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,8) | Уязвимость ядра операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить конфиденциальную информацию или обойти механизмы защиты |
| Уязвимость кода | 06.01.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции prctl\_vma\_anon\_name ядра операционной системы Android связана с отсутствием процедуры проверки доступности областей виртуальной памяти для обновления. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии или вызвать отказ в обслуживании с помощью специально созданного приложения |
| Уязвимость кода | 06.01.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость приложения Widevine QSEE TrustZone операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения, использующего QSEECOM |
| Уязвимость кода | 06.01.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера Imagination Technologies операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 06.01.2016 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера MediaTek misc-sd операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.12.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость медиасервера операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (повреждение памяти) |
| Уязвимость кода | 09.12.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость медиасервера операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (повреждение памяти) |
| Уязвимость кода | 09.12.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость медиасервера операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании (повреждение памяти) |
| Уязвимость кода | 09.12.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера дисплея операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) при помощи специально сформированного медиа файла |
| Уязвимость кода | 09.12.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость драйвера дисплея операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) при помощи специально сформированного медиа файла |
| Уязвимость кода | 09.12.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента Wi-Fi операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.12.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента SystemUI операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.12.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.12.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость ядра операционной системы Android связана с недостатками разграничения доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 09.12.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента Skia операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) при помощи специально сформированного медиа файла |
| Уязвимость кода | 09.12.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента mediaserver операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) при помощи специально сформированного медиа файла |
| Уязвимость кода | 03.11.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libmedia операционной системы Android связана с недостатками разграничения доступа к файлам. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально созданного приложения |
| Уязвимость кода | 03.11.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libstagefright операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии или вызвать отказ в обслуживании с помощью специально созданного приложения |
| Уязвимость кода | 06.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость подсистемы Runtime операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально сформированного приложения |
| Уязвимость кода | 06.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента Media Player Framework операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально сформированного приложения |
| Уязвимость кода | 06.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента mediaserver операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально сформированного приложения |
| Уязвимость кода | 06.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость плагина Secure Element Evaluation Kit операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально сформированного приложения |
| Уязвимость кода | 06.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента mediaserver операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, повысить свои привилегии с помощью специально сформированного приложения |
| Уязвимость кода | 02.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libutils операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код с помощью специально сформированных метаданных MP3 или MP4-файла |
| Уязвимость кода | 02.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость библиотеки libstagefright операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код с помощью специально сформированных заголовков MP3 или MP4-файла |
| Уязвимость кода | 01.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Множественные уязвимости компонента Keystore операционной системы Android связаны с переполнением буфера в динамической памяти, вызванным целочисленным переполнением. Эксплуатация уязвимостей может позволить нарушителю, действующему удалённо, выполнить произвольный код и читать произвольные ключи Keystore с помощью специально сформированного приложения |
| Уязвимость архитектуры | 01.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) | Уязвимость компонента Lockscreen операционной системы Android связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему локально, получить доступ к системе из-за отсутствия ограничений на длину пароля, что позволяет вызвать отказ приложения путем ввода большого количества символов |
| Уязвимость кода | 01.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции checkDestination операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, обойти процедуру подтверждения личности путем отправки короткого SMS-сообщения с помощью специально сформированного приложения |
| Уязвимость кода | 01.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции Region\_createFromParcel операционной системы Android связана с недостатками разграничения доступа к некоторым функциям. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код с помощью специально сформированного приложения |
| Уязвимость кода | 01.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента SIM Toolkit операционной системы Android связана с недостатками разграничения доступа к файлам. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, перехватывать или эмулировать SIM STK команды с помощью специально сформированного приложения |
| Уязвимость кода | 01.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Множественные уязвимости библиотеки libeffects операционной системы Android вызваны переполнением буфера в динамической памяти. Эксплуатация уязвимостей может позволить нарушителю, действующему удалённо, выполнить произвольный код с помощью специально сформированного приложения |
| Уязвимость кода | 01.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость класса OpenSSLX509Certificate модуля org/conscrypt/OpenSSLX509Certificate.java операционной системы Android существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код с помощью специально сформированного приложения |
| Уязвимость кода | 01.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции OMXNodeInstance::emptyBuffer библиотеки libstagefright операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код с помощью специально сформированного приложения |
| Уязвимость кода | 01.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции readAt службы mediaserver операционной системы Android вызвана переполнением буфера. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код с помощью специально сформированного приложения |
| Уязвимость кода | 01.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции MPEG4Extractor::parseChunk библиотеки libstagefright операционной системы Android связана с целочисленным переполнением. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код или вызвать отказ в обслуживании с помощью специально сформированных данных в формате MPEG-4 |
| Уязвимость кода | 01.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 8,5) | Уязвимость функции Bitmap\_createFromParcel (libcutils/native\_handle.c) операционной системы Android связана с целочисленным переполнением. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании или получить доступ к информации в памяти устройства с помощью специально сформированного приложения |
| Уязвимость кода | 01.10.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость функции native\_handle\_create (libcutils/native\_handle.c) операционной системы Android связана с целочисленным переполнением. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить привилегии различных приложений или вызвать отказ в обслуживании с помощью специально сформированного приложения |
| Уязвимость кода | 27.04.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 9,3) | Уязвимость компонента media\_server (IHDCP.cpp) операционной системы Android вызвана целочисленным переполнением. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код с помощью специально созданного приложения |
| Уязвимость кода | 06.02.2015 | Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,1) | Уязвимость компонента media\_server операционной системы Android вызвана целочисленным переполнением. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании с помощью специально созданного приложения |

