# CVE Detail – CVE-2017-8252

Kernel can inject faults in computations during the execution of TrustZone leading to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9615, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, SM7150, Snapdragon\_High\_Med\_2016, SXR1130

## Threat-Mapped Scoring

Score: 2.3

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.11029

## CVSS Scoring

CVSS v3.0 Score: 5.5

Severity: MEDIUM

## Mapped CWE(s)

* CWE-285: Improper Authorization

## CAPEC(s)

* CAPEC-1: Accessing Functionality Not Properly Constrained by ACLs
* CAPEC-104: Cross Zone Scripting
* CAPEC-127: Directory Indexing
* CAPEC-13: Subverting Environment Variable Values
* CAPEC-17: Using Malicious Files
* CAPEC-39: Manipulating Opaque Client-based Data Tokens
* CAPEC-402: Bypassing ATA Password Security
* CAPEC-45: Buffer Overflow via Symbolic Links
* CAPEC-5: Blue Boxing
* CAPEC-51: Poison Web Service Registry
* CAPEC-59: Session Credential Falsification through Prediction
* CAPEC-60: Reusing Session IDs (aka Session Replay)
* CAPEC-647: Collect Data from Registries
* CAPEC-668: Key Negotiation of Bluetooth Attack (KNOB)
* CAPEC-76: Manipulating Web Input to File System Calls
* CAPEC-77: Manipulating User-Controlled Variables
* CAPEC-87: Forceful Browsing

## ATT&CK Techniques

* T1574.007: Path Interception by PATH Environment Variable
* T1552.002: Credentials in Registry
* T1005: Data from Local System
* T1574.006: Dynamic Linker Hijacking
* T1574.005: Executable Installer File Permissions Weakness
* T1083: File and Directory Discovery
* T1134.001: Token Impersonation/Theft
* T1562.003: Impair Command History Logging
* T1574.010: Services File Permissions Weakness
* T1012: Query Registry
* T1550.004: Web Session Cookie
* T1565.002: Transmitted Data Manipulation

## Used By (Actors/Tools)

* TrickBot (malware)
* PowerDuke (malware)
* BLINDINGCAN (malware)
* Ninja (malware)
* RCSession (malware)
* QuietSieve (malware)
* SynAck (malware)
* Bumblebee (malware)
* AcidRain (malware)
* Amadey (malware)
* Proxysvc (malware)
* Orz (malware)
* yty (malware)
* Backdoor.Oldrea (malware)
* Stuxnet (malware)
* AvosLocker (malware)
* POWRUNER (malware)
* KOPILUWAK (malware)
* COATHANGER (malware)
* Sardonic (malware)
* Smoke Loader (malware)
* WindTail (malware)
* Misdat (malware)
* KEYMARBLE (malware)
* Ursnif (malware)
* ThreatNeedle (malware)
* RansomHub (malware)
* ZLib (malware)
* RedLeaves (malware)
* POWERSOURCE (malware)
* LITTLELAMB.WOOLTEA (malware)
* Zeus Panda (malware)
* GeminiDuke (malware)
* FrameworkPOS (malware)
* GravityRAT (malware)
* Prestige (malware)
* Bankshot (malware)
* SharpDisco (malware)
* StrongPity (malware)
* xCaon (malware)
* WinMM (malware)
* Nebulae (malware)
* AuditCred (malware)
* Kasidet (malware)
* OceanSalt (malware)
* Playcrypt (malware)
* Brave Prince (malware)
* RainyDay (malware)
* AppleSeed (malware)
* NETWIRE (malware)
* TinyTurla (malware)
* CosmicDuke (malware)
* EnvyScout (malware)
* Gomir (malware)
* Aria-body (malware)
* Emotet (malware)
* BOLDMOVE (malware)
* Crimson (malware)
* Tomiris (malware)
* TEARDROP (malware)
* DUSTTRAP (malware)
* Turian (malware)
* BADHATCH (malware)
* Machete (malware)
* PowerLess (malware)
* Action RAT (malware)
* Avenger (malware)
* Prikormka (malware)
* PingPull (malware)
* WellMess (malware)
* Dacls (malware)
* DropBook (malware)
* Woody RAT (malware)
* Mafalda (malware)
* ELMER (malware)
* AuTo Stealer (malware)
* Hildegard (malware)
* SombRAT (malware)
* ODAgent (malware)
* FLASHFLOOD (malware)
* FlawedAmmyy (malware)
* FYAnti (malware)
* LoFiSe (malware)
* HOPLIGHT (malware)
* Cuckoo Stealer (malware)
* MobileOrder (malware)
* WastedLocker (malware)
* InvisiMole (malware)
* P.A.S. Webshell (malware)
* Volgmer (malware)
* WINERACK (malware)
* WhisperGate (malware)
* FruitFly (malware)
* AcidPour (malware)
* Skidmap (malware)
* Okrum (malware)
* TRANSLATEXT (malware)
* Line Dancer (malware)
* Neoichor (malware)
* Conti (malware)
* Raspberry Robin (malware)
* Mispadu (malware)
* Megazord (malware)
* Diavol (malware)
* Doki (malware)
* Siloscape (malware)
* BlackCat (malware)
* Fysbis (malware)
* MarkiRAT (malware)
* Kazuar (malware)
* NETEAGLE (malware)
* POORAIM (malware)
* CHIMNEYSWEEP (malware)
* FatDuke (malware)
* Lucifer (malware)
* BlackEnergy (malware)
* zwShell (malware)
* DRATzarus (malware)
* Rising Sun (malware)
* NotPetya (malware)
* ShimRat (malware)
* Chrommme (malware)
* BADFLICK (malware)
* ObliqueRAT (malware)
* SHOTPUT (malware)
* Avaddon (malware)
* Flagpro (malware)
* SpicyOmelette (malware)
* XAgentOSX (malware)
* Green Lambert (malware)
* China Chopper (malware)
* LightSpy (malware)
* Cheerscrypt (malware)
* KeyBoy (malware)
* MiniDuke (malware)
* Pteranodon (malware)
* ROKRAT (malware)
* Babuk (malware)
* Exbyte (malware)
* DarkWatchman (malware)
* BlackMould (malware)
* PACEMAKER (malware)
* BBSRAT (malware)
* PlugX (malware)
* Reaver (malware)
* Bisonal (malware)
* MultiLayer Wiper (malware)
* DustySky (malware)
* Remsec (malware)
* Rover (malware)
* Epic (malware)
* LightNeuron (malware)
* Peppy (malware)
* Cuba (malware)
* DEATHRANSOM (malware)
* Clambling (malware)
* Akira (malware)
* DarkGate (malware)
* Mongall (malware)
* LockBit 3.0 (malware)
* SVCReady (malware)
* FoggyWeb (malware)
* Carbanak (malware)
* Hydraq (malware)
* CreepyDrive (malware)
* Caterpillar WebShell (malware)
* Elise (malware)
* USBferry (malware)
* WannaCry (malware)
* TSCookie (malware)
* Latrodectus (malware)
* Saint Bot (malware)
* CharmPower (malware)
* TYPEFRAME (malware)
* 3PARA RAT (malware)
* Mori (malware)
* QUADAGENT (malware)
* TAINTEDSCRIBE (malware)
* Royal (malware)
* BendyBear (malware)
* Uroburos (malware)
* Metamorfo (malware)
* Spica (malware)
* Trojan.Karagany (malware)
* Bandook (malware)
* TINYTYPHON (malware)
* KONNI (malware)
* RAPIDPULSE (malware)
* gh0st RAT (malware)
* Shamoon (malware)
* DnsSystem (malware)
* CORALDECK (malware)
* SPACESHIP (malware)
* BLUELIGHT (malware)
* KGH\_SPY (malware)
* down\_new (malware)
* Ixeshe (malware)
* Micropsia (malware)
* RARSTONE (malware)
* BPFDoor (malware)
* Black Basta (malware)
* StoneDrill (malware)
* 4H RAT (malware)
* Attor (malware)
* LitePower (malware)
* MegaCortex (malware)
* StreamEx (malware)
* BoxCaon (malware)
* NightClub (malware)
* Crutch (malware)
* Akira \_v2 (malware)
* SDBbot (malware)
* RTM (malware)
* QUIETCANARY (malware)
* Derusbi (malware)
* BlackByte Ransomware (malware)
* SodaMaster (malware)
* Hikit (malware)
* StrelaStealer (malware)
* WellMail (malware)
* LiteDuke (malware)
* RawPOS (malware)
* Sibot (malware)
* ZxxZ (malware)
* Tarrask (malware)
* WINDSHIELD (malware)
* Drovorub (malware)
* Shark (malware)
* Bazar (malware)
* BadPatch (malware)
* MESSAGETAP (malware)
* RATANKBA (malware)
* SUGARDUMP (malware)
* SOUNDBITE (malware)
* MoonWind (malware)
* Ryuk (malware)
* Cryptoistic (malware)
* HermeticWiper (malware)
* MgBot (malware)
* ccf32 (malware)
* Kapeka (malware)
* LockBit 2.0 (malware)
* Zebrocy (malware)
* FinFisher (malware)
* LunarMail (malware)
* CrossRAT (malware)
* OwaAuth (malware)
* Cobalt Strike (malware)
* SUNBURST (malware)
* HotCroissant (malware)
* REvil (malware)
* Valak (malware)
* Samurai (malware)
* PinchDuke (malware)
* Milan (malware)
* USBStealer (malware)
* OSX\_OCEANLOTUS.D (malware)
* Taidoor (malware)
* Kivars (malware)
* CaddyWiper (malware)
* Cyclops Blink (malware)
* PoisonIvy (malware)
* Seasalt (malware)
* TajMahal (malware)
* PLEAD (malware)
* Raccoon Stealer (malware)
* IPsec Helper (malware)
* Carbon (malware)
* Cardinal RAT (malware)
* DanBot (malware)
* Calisto (malware)
* Pisloader (malware)
* GoldenSpy (malware)
* Gold Dragon (malware)
* Ramsay (malware)
* Carberp (malware)
* Pillowmint (malware)
* MacMa (malware)
* FunnyDream (malware)
* ROADSWEEP (malware)
* SUNSPOT (malware)
* SysUpdate (malware)
* OutSteel (malware)
* BackConfig (malware)
* Kwampirs (malware)
* BoomBox (malware)
* PUNCHTRACK (malware)
* Mango (malware)
* InnaputRAT (malware)
* GrimAgent (malware)
* LookBack (malware)
* Clop (malware)
* Lokibot (malware)
* PoetRAT (malware)
* CHOPSTICK (malware)
* StealBit (malware)
* FELIXROOT (malware)
* ZxShell (malware)
* SLIGHTPULSE (malware)
* NDiskMonitor (malware)
* DDKONG (malware)
* Penquin (malware)
* BabyShark (malware)
* Cannon (malware)
* Melcoz (malware)
* Winnti for Windows (malware)
* Troll Stealer (malware)
* BLACKCOFFEE (malware)
* Ebury (malware)
* Kinsing (malware)
* njRAT (malware)
* ZIPLINE (malware)
* ComRAT (malware)
* ChChes (malware)
* Manjusaka (malware)
* IceApple (malware)
* JPIN (malware)
* metaMain (malware)
* SideTwist (malware)
* Psylo (malware)
* Heyoka Backdoor (malware)
* HTTPBrowser (malware)
* Mis-Type (malware)
* LunarWeb (malware)
* XCSSET (malware)
* Octopus (malware)
* KillDisk (malware)
* SoreFang (malware)
* STARWHALE (malware)
* Industroyer (malware)
* DownPaper (malware)
* Pcexter (malware)
* Kevin (malware)
* Agent Tesla (malware)
* Pasam (malware)
* POWERSTATS (malware)
* BADNEWS (malware)
* Linfo (malware)
* Goopy (malware)
* Remexi (malware)
* QakBot (malware)
* CookieMiner (malware)
* Gelsemium (malware)
* jRAT (malware)
* OSX/Shlayer (malware)
* Denis (malware)
* INC Ransomware (malware)
* Waterbear (malware)
* FIVEHANDS (malware)
* AutoIt backdoor (malware)
* OSInfo (malware)
* Dtrack (malware)
* Azorult (malware)
* BitPaymer (malware)
* BACKSPACE (malware)
* Zox (malware)
* UPPERCUT (malware)
* ADVSTORESHELL (malware)
* StrifeWater (malware)
* HiddenWasp (malware)
* WarzoneRAT (malware)
* SLOTHFULMEDIA (malware)
* FALLCHILL (malware)
* RemoteUtilities (tool)
* NPPSPY (tool)
* Sliver (tool)
* SILENTTRINITY (tool)
* PowerSploit (tool)
* Empire (tool)
* PcShare (tool)
* PoshC2 (tool)
* Rclone (tool)
* Brute Ratel C4 (tool)
* Remcos (tool)
* Out1 (tool)
* Imminent Monitor (tool)
* Forfiles (tool)
* MCMD (tool)
* cmd (tool)
* esentutl (tool)
* CrackMapExec (tool)
* Koadic (tool)
* Pupy (tool)
* Reg (tool)
* QuasarRAT (tool)
* Wevtutil (tool)
* Indrik Spider (intrusion-set)
* LuminousMoth (intrusion-set)
* Operation Wocao (campaign)
* Wizard Spider (intrusion-set)
* FIN7 (intrusion-set)
* Velvet Ant (intrusion-set)
* ArcaneDoor (campaign)
* Dragonfly (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* SolarWinds Compromise (campaign)
* Lazarus Group (intrusion-set)
* Aquatic Panda (intrusion-set)
* Daggerfly (intrusion-set)
* Inception (intrusion-set)
* admin@338 (intrusion-set)
* Operation CuckooBees (campaign)
* Play (intrusion-set)
* Sandworm Team (intrusion-set)
* Turla (intrusion-set)
* Ember Bear (intrusion-set)
* CostaRicto (campaign)
* TeamTNT (intrusion-set)
* FIN6 (intrusion-set)
* Patchwork (intrusion-set)
* APT28 (intrusion-set)
* Aoqin Dragon (intrusion-set)
* Darkhotel (intrusion-set)
* Ke3chang (intrusion-set)
* Volt Typhoon (intrusion-set)
* Leafminer (intrusion-set)
* Magic Hound (intrusion-set)
* APT29 (intrusion-set)
* Operation Honeybee (campaign)
* Andariel (intrusion-set)
* HAFNIUM (intrusion-set)
* APT39 (intrusion-set)
* MuddyWater (intrusion-set)
* APT38 (intrusion-set)
* APT32 (intrusion-set)
* BRONZE BUTLER (intrusion-set)
* APT5 (intrusion-set)
* Kimsuky (intrusion-set)
* Mustang Panda (intrusion-set)
* LAPSUS$ (intrusion-set)
* Chimera (intrusion-set)
* ToddyCat (intrusion-set)
* menuPass (intrusion-set)
* Tropic Trooper (intrusion-set)
* Operation Dream Job (campaign)
* Stealth Falcon (intrusion-set)
* APT37 (intrusion-set)
* APT41 (intrusion-set)
* FIN13 (intrusion-set)
* GALLIUM (intrusion-set)
* C0015 (campaign)
* Winnti Group (intrusion-set)
* FIN8 (intrusion-set)
* Rocke (intrusion-set)
* Scattered Spider (intrusion-set)
* CURIUM (intrusion-set)
* Windigo (intrusion-set)
* RedCurl (intrusion-set)
* Frankenstein (campaign)
* Sidewinder (intrusion-set)
* Confucius (intrusion-set)
* BlackByte (intrusion-set)
* Threat Group-3390 (intrusion-set)
* Gamaredon Group (intrusion-set)
* Night Dragon (campaign)
* Agrius (intrusion-set)
* Sea Turtle (intrusion-set)
* Axiom (intrusion-set)
* Dark Caracal (intrusion-set)
* APT3 (intrusion-set)
* Operation MidnightEclipse (campaign)
* ZIRCONIUM (intrusion-set)
* APT1 (intrusion-set)
* Sowbug (intrusion-set)
* HomeLand Justice (campaign)
* C0017 (campaign)
* Winter Vivern (intrusion-set)
* Cutting Edge (campaign)
* Lotus Blossom (intrusion-set)
* APT18 (intrusion-set)
* KV Botnet Activity (campaign)
* Star Blizzard (intrusion-set)
* C0026 (campaign)

## Affected Products

* cpe:2.3:o:qualcomm:ipq4019\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:ipq8074\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:mdm9150\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:mdm9206\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:mdm9607\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:mdm9615\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:mdm9635m\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:mdm9640\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:mdm9650\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:mdm9655\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:msm8909w\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:msm8996au\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:qca8081\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:qcs605\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:qc\_215\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_210\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_212\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_205\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_410\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_412\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_425\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_427\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_430\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_435\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_439\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_429\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_450\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_615\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_616\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_415\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_625\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_632\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_636\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_650\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_652\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_675\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_712\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_710\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_670\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_820\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_820a\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_835\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_845\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_850\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_855\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sd\_8cx\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sda660\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sdm439\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sdm630\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sdm660\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sdx20\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sdx24\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sm7150\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:snapdragon\_high\_med\_2016\_firmware:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:qualcomm:sxr1130\_firmware:-:\*:\*:\*:\*:\*:\*:\*