CENTER FOR CYBERSIKKERHED

Dato: 9. august 2016
Trusselsvurderingsenheden

Trusselsvurdering: ”QuadRooter” sårbarhed i Android-enheder med Qualcomm processorchips.

Formålet med denne trusselsvurdering er at varsle om sårbarheder i android-baserede smartphones og tablets, som benytter processorchips fra Qualcomm. Sårbarhederne betyder, at en aktør - via en app med ondsindet kode - kan opnå fuld kontrol med enheden.

Trusselsvurderingen er rettet mod brugere af Android-baserede enheder.

Hovedvurdering

- CFCS vurderer, at det er meget sandsynligt, at ondsindede aktører vil forsøge at udnytte sårbarhederne.
- CFCS vurderer, at hovedparten af producenterne af de berørte Android-enheder endnu ikke har udsendt sikkerhedsopdateringer, som fjerner alle sårbarhederne.
- Hvis anbefalingerne i denne trusselsvurdering følges, vurderer CFCS, at truslen mod danske slutbrugere på baggrund af sårbarhederne er LAV.

Analyse

Sårbarheden

Den 7. august 2016 blev der på internettet offentliggjort en række sårbarheder, som er navngivet ”QuadRooter”. Sårbarhederne findes i software, som er installeret på Android-enheder, som benytter Qualcomm processorchips. Sårbarhederne kan udnyttes af en aktør, som via en app med ondsindet kode kan opnå fuld kontrol med enheden og dermed også få adgang til de data, som ligger på enheden. En app med ondsindet kode vil ikke have behov for særlige rettigheder på enheden for at kunne udnytte sårbarhederne.

Hvis en Android-enhed først er blevet inficeret via disse sårbarheder, vil det højst sandsynligt ikke være tilstrækkeligt at afinstallere app'en for at fjerne inficeringen. En komplet fjernelse vil formentlig kræve en gen-installering af styresystemet på enheden.

På internettet er det muligt at finde yderligere information om sårbarhederne, fx via http://blog.checkpoint.com/2016/08/07/quadrooter/

Hvilke enheder er sårbare

Sårbarhederne omfatter potentielt alle Android-enheder, som benytter Qualcomm processor-chips. Eksempler på producenter som benytter disse processor-chips er: BlackBerry, Blackphone, Google Nexus, HTC, LG, Motorola, OnePlus, Samsung og Sony.

Sikkerhedsfirmaet CheckPoint har udsendt en app, som kan undersøge, om en specifik Android-enhed indeholder sårbarhederne. QuadRooter Scanner app'en kan downloades fra Google Play.

Udnyttelse af sårbarhederne

En række betingelser skal være opfyldt, for at en aktør kan have succes med at udnytte disse sårbarheder:

1. Aktøren skal have kompetencen til at designe kode, som udnytter sårbarhederne.
2. Aktøren skal designe en app, som indeholder den ondsindede kode. Alternativt kan aktøren implementere den ondsindede kode i en eksisterende app.
3. Aktøren skal gøre app'en tilgængelig via Google Play, alternativt via en uofficiel app-downloadkilde.
4. Brugeren af Android-enheden skal selv downloade og installere app'en, som indeholder den ondsindede kode.

Fjernelse af sårbarheden

Qualcomm har allerede udsendt sikkerhedsopdateringer til de producenter, som benytter deres processorchips. Disse opdateringer skal imidlertid implementeres i producenternes egne sikkerhedsopdateringer, inden de kan gøres tilgængelige for slutbrugerne. Dette betyder, at der vil gå længere tid (evt. uger og måneder), inden der er sikkerhedsopdateringer til rådighed for alle berørte enheder. Endvidere er det sandsynligt, at der vil være ældre enheder, som producenterne ikke længere udsender opdateringer til.

Hvordan skal brugerne forholde sig?

Det er vigtigt at bemærke, at udnyttelsen af disse sårbarheder kræver, at brugeren selv installerer en app, som indeholder kode, der udnytter sårbarhederne. Derfor anbefales det at være kritisk overfor, hvilke apps som downloades - og udelukkende downloade apps fra Google Play.

Udviklere, som får apps udgivet via Google Play, er registreret af Google, og bliver ranglistet i

forhold til kvalitet og sikkerhed, ligesom eventuelt ondsindede apps løbende bliver fjernet fra Google Play.

Endelig skal brugeren sørge for løbende at installere de softwareopdateringer, som udsendes til deres smartphone eller tablet.

FE bruger denne skala for sandsynlighed i analyser: