CENTER FOR CYBERSIKKERHED

Dato: 6. april 2016
Sektion: CPT05

Cybervurdering: Truslen fra ”Stagefright” sårbarheden i Android styresystemet

Formålet med vurderingen er at varsle om en sårbarhed i Android styresystemet. Dette styresystem er det mest udbredte til smartphones og tablets, med en markedsandel som i 2014 blev anslået til 78 %. Udnyttelse af sårbarheder i dette styresystem vil kunne berøre mange mennesker – også i Danmark.

Hovedvurdering

- Op mod 98 % af alle smartphones og tablets baseret på Android styresystemet er sårbare overfor udnyttelse af den såkaldte ”Stagefright” sårbarhed.

- FE vurderer, at denne sårbarhed endnu ikke er udnyttet af kriminelle, men efter at mulighederne for at udnytte det er blevet offentliggjort, er det sandsynligt, at sårbarheden vil blive forsøgt udnyttet indenfor de næste måneder.

- Hvis slutbrugeren af enheder med Android styresystemet følger de almindelige retningslinjer for sikker brug af smartphones, som angivet i dette dokument, er inficering via denne sårbarhed ikke sandsynlig.

- FE vurderer, at truslen fra udnyttelse af sårbarheden er **LAV.**

Analyse

Den såkaldte ”Stagefright” sårbarhed i Android styresystemet, blev offentliggjort af sikkerhedsfirmaet Zimperium i juli 2015. Sårbarheden betyder, at det er muligt at inficere en Android-enhed som benytter Android styresystemet, f.eks. en smartphone, tablet, TV eller mini-pc, med malware via en modificeret MPEG video-fil.

Sårbarheden findes i den del af Android koden, som håndterer afspilning af video-filer. Inficering af en Android enhed kan derfor ske ved modtagelse af en MMS eller e-mail med en vedhæftet modificeret video-fil. Det kan også ske ved at brugeren besøger en ondsindet eller hacket hjemmeside, og der downloader eller afspiller en modificeret video-fil.

Inficering af Android enheden kræver ikke at video-filen afspilles – blot at den modtages eller downloades.

Det som gør denne sårbarhed specielt interessant nu er, at der i marts 2016 blev offentliggjort et whitepaper, som beskriver hvorledes "Stagefright" sårbarheden kan udnyttes.
Det skal dog bemærkes, at dette whitepaper ikke er et færdigt exploit, som kriminelle umiddelbart kan anvende til et angreb. Det er en analyse af de mulige metoder, som kan anvendes for at udnytte sårbarheden. Der udestår således et større arbejde, som kræver personer med ekspertviden indenfor området, før deciderede angreb kan udføres.

Sårbarhedens udbredelse
"Stagefright" er en samlet betegnelse for et antal identificerede sårbarheder, såkaldte CVE'er (Common Vulnerabilities and Exposures), i Android styresystemet.
Sårbarhederne findes i Android versionerne 2.2 til 5.1, som udgør 98 % af de Android versioner som er i brug. I versionerne 4.0 til 5.1 er der imidlertid implementeret en sikkerhedsfunktion, som gør det vanskeligere at udnytte sårbarhederne. Denne sikkerhedsfunktion kaldes ASLR (Address Space Layout Randomization), og betyder, at angreb skal tilpasses den specifikke smartphone model for at være effektivt. Android versionerne 4.0 til 5.1 anvendes i dag i omkring 95 % af Android-enhederne.

Den seneste Android version 6.0 indeholder ikke "Stagefright" sårbarheden.

Sikkerhedsopdateringer til Android
Google, som står bag Android styresystemet, udgav i oktober 2015, de første sikkerhedsopdateringer imod denne sårbarhed, som er stillet til rådighed for mobilfabrikanterne. Der er siden udgivet flere opdateringer.

Da der findes mange varianter af Android systemet, og da der er mange fabrikanter af Android-enheder, som skal have opdateret deres firmware, og derefter sendt opdateringerne ud til slutbrugerne, kan det erfaringsmæssigt tage lang tid, før den enkelte enhed er opdateret. Endelig er der fabrikanter, som slet ikke sender opdateringer ud til deres ældre modeller med ældre versioner af Android styresystemet.

Hvis man ønsker at kontrollere, om en specifik Android enhed er eksponeret for "Stagefright" sårbarheden, så har Zimperium udgivet en app i Google Play kaldet "Stagefright Detector". Denne

app kan undersøge, om den specifikke Android-enhed indeholder nogle af de sårbarheder, som relaterer sig til "Stagefright" sårbarheden.

Den konkrete trussel

Da sårbarheden er teknisk vanskelig at udnytte i praksis for 95 % af Android-enhederne i brug, og da Google har udgivet sikkerhedsopdateringer mod sårbarheden, som er på vej til, eller allerede er udsendt til slutbrugerne, er inficering via denne sårbarhed ikke sandsynlig, hvis slutbrugeren følger de almindelige retningslinjer for sikker brug af smartphones, som angivet nedenfor.

FE vurderer, at truslen fra udnyttelse af sårbarheden er **LAV.**

Mulige foranstaltninger for at mindske risikoen for inficering

Der er en række enkle forholdsregler, som enhver slutbruger bør tage, for at mindske risikoen for at smartphone eller tablet inficeres med malware. Disse forholdsregler vil også mindske risikoen for inficering via "Stagefright" sårbarheden:

<u>Generelle forholdsregler:</u>

1. Undlad at besøge ukendte hjemmesider, eller hjemmesider du ikke har tillid til.
2. Undlad at klikke på links som du modtager via e-mail, sms eller MMS, fra personer du ikke kender eller har tillid til.
3. Undlad at installere apps fra andre kilder end de officielle, "Google Play" for Android, og "App Store" for iPhone. Man bør sætte sin smartphone op, så den kun accepterer download af apps fra disse kilder.
4. Installer altid de sikkerhedsopdateringer som udsendes til din smartphone eller tablet, og konfigurer din enhed til automatisk at hente opdateringer.
5. Installer en anerkendt antivirus app på din smartphone eller tablet.

<u>Specifik forholdsregel målrettet "Stagefright" sårbarheden:</u>

6. Deaktiver automatisk hentning af MMS på din smartphone. Hvis du benytter flere apps til modtagelse af MMS beskeder, skal funktionen deaktiveres på dem alle. Efter deaktivering af automatisk hentning af MMS, vil du fremover få en notifikation om accept af download, hver gang du modtager en MMS. Her skal du naturligvis også følge de generelle forholdsregler, og kun downloade MMS'er fra personer du har tillid til.

FE bruger denne skala for sandsynlighed i analyser: