CENTER FOR CYBERSIKKERHED

Dato: 5. januar 2018
Opdateret: 10. januar 2018

Trusselsvurdering: Meltdown og Spectre gør computere sårbare over hele verden

Formålet med denne trusselsvurdering er at orientere om to sårbarheder ved computeres Central Processing Unit (CPU), som potentielt kan medføre alvorlige kompromitteringer af de systemer, CPU'erne sidder i. Det er vigtigt, at myndigheder og virksomheder følger denne vurderings anbefalinger.

Hovedvurdering

- En ondsindet aktør, som har opnået adgang til at eksekvere kode på en computer, kan udnytte sårbarhederne til at opnå uautoriseret adgang til data i computerens systemhukommelse.
- Det er sandsynligt, at ondsindede aktører vil udvikle exploits, som kan udnytte sårbarhederne, og det er meget sandsynligt, at ondsindede aktører vil forsøge at udnytte sårbarhederne.
- Det er muligt at udnytte sårbarhederne via et JavaScript på en hjemmeside. Metoden kræver, at brugeren aktivt besøger en ondsindet eller inficeret hjemmeside. Metoden kan give adgang til at læse systemhukommelsen på brugerens computer, men giver ikke adgang til at eksekvere ondsindet kode på computeren.
- På nuværende tidspunkt er sårbarhederne endnu ikke erkendt udnyttet.
- Da sårbarhederne alene ikke kan udnyttes til at opnå uautoriseret adgang til en computer via internettet, vurderer CFCS, at sårbarhederne ikke umiddelbart har kritisk betydning for samfundsvigtig infrastruktur i Danmark.
- CFCS anbefaler ejere og administratorer af it-systemer at sikre, at alle benyttede systemer opdateres med de seneste opdateringer fra leverandøren.
- Brugere af cloud-tjenester bør sikre sig, at leverandøren har taget forholdsregler mod sårbarhederne samt sørge for at opdateret de virtuelle maskiner, som brugeren eventuelt selv drifter.

Analyse

Trusselsvurderingen er en opdatering af tidligere trusselsvurdering udsendt den 5. januar 2017. CFCS følger løbende udviklingen, og vil opdatere trusselsvurderingen, hvis nye oplysninger giver anledning til væsentlige ændringer.

På internettet er der i denne uge offentliggjort oplysninger om nye sårbarheder i mange forskellige CPU'er, som anvendes i computere i dag. Sårbarheder er CVE-2017-5753 og CVE-2017-5715, som samlet kaldes Spectre, og CVE-2017-5754 som kaldes Meltdown.

På nuværende tidspunkt er Meltdown sårbarheden kun erkendt i Intel CPU'er, mens Spectre sårbarheden oprindeligt er fundet på CPU'er fra Intel, ARM og AMD. Det er meget sandsynligt, at også CPU'er fra andre producenter er omfattet af Spectre sårbarheden.

De sårbare CPU'er benyttes blandt andet i computere, servere, smartphones, tablets og netværksudstyr.

Antallet af CPU'er og dermed sårbare computere og lignende gør, at et effektivt exploit kan anvendes mod mange angrebsmål.

Sårbarhederne udnytter svagheder i de teknikker, som CPU producenterne benytter for at øge beregningshastigheden. Det er ikke umiddelbart muligt at udnytte sårbarhederne via internettet uden anden forudgående kompromittering. Det er dog muligt, at udnytte sårbarhederne via et JavaScript på en hjemmeside. En bruger, som besøger en ondsindet eller inficeret hjemmeside, som indeholder et sådan JavaScript, risikerer således, at en aktør får adgang til at læse systemhukommelsen i den anvendte computer. Leverandørerne af de mest anvendte operativsystemer og internetbrowsere har dog allerede udsendt sikkerhedsopdateringer, som imødegår denne trussel.

Sårbarhederne medfører, at en aktør, som allerede har adgang til at eksekvere kode på systemer med en sårbare CPU, har mulighed for at opnå adgang til systemhukommelsen, som er den særlige del af computerens hukommelse, som primært anvendes af operativsystemet. Sårbarhederne giver alene adgang til at læse det aktuelle indhold i systemhukommelsen, og giver ikke i sig selv adgang til at eksekvere kommandoer på computeren, men aktøren kan potentielt få adgang til følsomme data som kodeord og lignende, som ligger i systemhukommelsen.

Ved brug af en cloud-tjeneste er det potentielt muligt for en ondsindet bruger at få adgang til data, som befinder sig på en virtuel maskine, som benyttes af en anden kunde. Flere af de store leverandører af cloud-tjenester har allerede opdateret deres systemer for at imødegå disse sårbarheder.

På nuværende tidspunkt er sårbarhederne endnu ikke erkendt udnyttet.

Anbefaling

Sårbarhederne har været kendt af nogle CPU producenter og software leverandører siden juni 2017, og flere leverandører af operativsystemer og internetbrowsere har allerede udsendt sikkerhedsopdateringer, som imødegår sårbarhederne. CFCS anbefaler ejere og administratorer af it-systemer at sikre, at alle benyttede systemer opdateres med de seneste opdateringer fra leverandøren. Der vil i den kommende tid løbende blive udgivet nye softwareopdateringer, så der vil være behov for kontinuerligt at være opmærksom på seneste version på de berørte systemer.

Generelt bør alle it-ansvarlige løbende holde sig orienteret via leverandører og internettet om sårbarhederne og anbefalede mitigeringer.
Brugere af cloud-tjenester bør sikre sig, at leverandøren har opdateret sine systemer for at imødegå sårbarhederne. Ofte vil denne information være tilgængelig via leverandørens hjemmeside. Endvidere skal brugeren sørge for selv at opdatere de virtuelle maskiner, som brugeren eventuelt selv har driftsansvar for.

Der opdages konstant nye sårbarheder i software og it-systemer. Hvis leverandøren ikke løbende udsender sikkerhedsopdateringer, som fjerner disse sårbarheder, eller hvis brugeren ikke implementerer disse sikkerhedsopdateringer, vil softwaren eller it-systemet udgøre en større og større sikkerhedsrisiko for brugeren.

CFCS anbefaler generelt virksomheder og myndigheder til ikke at benytte software og hardware, som ikke længere modtager sikkerhedsopdateringer fra leverandøren. Dette gælder især i de tilfælde, hvor de pågældende systemer kan nås via internettet.

FE bruger denne skala for sandsynlighed i analyser: