CENTER FOR CYBERSIKKERHED

Dato: 1. februar 2017

Trusselsvurdering: Sårbarhed i Cisco WebEx browserudvidelse

Cisco WebEx benyttes af mange danske virksomheder til afvikling af online møder. Visse versioner af browserudvidelser for Cisco WebEx indeholder imidlertid en sårbarhed, som gør det muligt for en angriber at kompromittere computere, hvor Cisco WebEx er installeret.

Hovedvurdering

- Det er sandsynligt, at ondsindede aktører vil forsøge at udnytte sårbarheden.
- Cisco har udgivet opdateringer, som fjerner sårbarheden, og de fleste sårbare browserudvidelser vil automatisk blive opdateret, næste gang brugeren benytter WebEx. Derfor vurderer CFCS, at truslen for en kompromittering via denne sårbarhed er **LAV**.
- CFCS anbefaler imidlertid alle ejere og administratorer af Windowsbaserede computere, som benytter Cisco WebEx, til snarest muligt at undersøge om den benyttede version af Cisco WebEx browserudvidelse er sårbar, og snarest muligt at opdatere til en ikke-sårbar version.

Analyse

Cisco har den 31. januar opdateret en Cisco Security Advisory angående sårbarheder i deres Cisco WebEx browserudvidelser.

Sårbarheden, som blev omtalt første gang den 21. januar 2017, gør det muligt for en angriber, at kompromittere en internetbrowser som indeholder en sårbar Cisco WebEx browserudvidelse. Når internetbrowseren først er kompromitteret, vil det også være muligt for angriberen at kompromittere den pågældende computer.

Sårbarheden eksisterer kun i computere som benytter et Microsoft Windows operativsystem.

Ifølge Cisco findes sårbarheden i Cisco WebEx browserudvidelser til Google Chrome, Firefox og Internet Explorer, men ikke i Microsoft Edge.

Sårbarheden er relativ let at udnytte, og kræver blot, at offeret besøger en hjemmeside, som kontrolleres af angriberen.

Det er på internettet muligt at finde oplysninger om, hvorledes sårbarheden kan anvendes til at kompromittere en computer. Dette betyder, at det er sandsynligt, at der er aktører som vil forsøge at udnytte sårbarheden.

WebEx browserudvidelsen vil imidlertid, i de fleste tilfælde, automatisk blive opdateret til en ikke-sårbar version næste gang brugeren benytter WebEx. Derfor vurderer CFCS, at truslen fra kompromittering via denne sårbarhed er **LAV**.

Identificering og fjernelse af sårbarheden
Cisco har udgivet et såkaldt Cisco Security Advisory (cisco-sa-20170124-webex), som beskriver sårbarheden, hvilke versioner af browserudvidelser som er sårbare, samt hvorledes brugeren identificerer, om den benyttede version af Cisco WebEx er sårbar.

Cisco Security Advisory indeholder også oplysninger om mulige mitigerende foranstaltninger, samt vejledning til opdatering til en ikke-sårbar version.

Den aktuelle Cisco Security Advisory kan findes via dette link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170124-webex

Anbefaling
De fleste brugere vil opleve, at WebEx browserudvidelsen automatisk opdateres til en ikke-sårbar version. Imidlertid kan der være tilfælde, hvor dette ikke sker, f.eks. hvis brugeren ikke har administrative rettigheder til computeren.

CFCS anbefaler alle administratorer og brugere af computere, som benyttes til Cisco WebEx online møder, til snarest muligt at undersøge, om den benyttede browserudvidelse til WebEx er sårbar, og i pågældende tilfælde hurtigst muligt at opdatere til en ikke-sårbar version.

Virksomheder og myndigheder kan vælge at blokere for udnyttelse af sårbarheden via en URL-filtrering. Yderligere information om dette findes i ovenstående Cisco Security Advisory.

FE bruger denne skala for sandsynlighed i analyser: