CENTER FOR CYBERSIKKERHED

Dato: 18. august 2016
Trusselsvurderingsenheden

Trusselsvurdering: Nye sårbarheder i Cisco firewall er blevet offentliggjort

Formålet med denne trusselsvurdering er at varsle om netop offentliggjort kode, som udnytter sårbarheder i firewalls fra Cisco. Firewalls fra andre producenter er også berørt af offentliggørelsen af kode som udnytter andre sårbarheder. Sårbarhederne vurderes til at være alvorlige.
Trusselsvurderingen er primært rettet mod administratorer af Cisco firewalls.

Hovedvurdering

- CFCS vurderer, at sårbarhederne udgør en trussel mod de formentlig talrige myndigheder og virksomheder, som benytter sårbare Cisco firewalls.
- Dele af angrebskoden muliggør etablering af en permanent bagdør i Cisco firewalls.
- CFCS vurderer, at det er meget sandsynligt, at der er aktører som på kort sigt vil forsøge at udnytte sårbarhederne.
- CFCS anbefaler alle brugere af Cisco firewalls at undersøge, om deres produkt er omfattet af disse sårbarheder, og i pågældende tilfælde kontakte deres leverandør, samt følge anbefalingerne fra Cisco.

Analyse

Sårbarhederne

Den 17. august 2016 udsendte Cisco en såkaldt Event Response med betegnelsen ERP-56516. Udsendelsen var en reaktion på, at en gruppe som kalder sig ”The Shadow Brokers”, få dage før havde offentliggjort kode, som udnytter sårbarheder i Cisco firewalls. Der er endnu ikke rettelser tilgængelig for alle sårbarheder.

Gruppen har også offentliggjort kode, som angiveligt kan benyttes til at angribe firewalls fra producenterne Fortigate, Topsec, WatchGuard og Juniper. Det er i skrivende stund ikke klart, hvorvidt produkter fra disse producenter er sårbare overfor den offentliggjorte kode.

Flere af angrebene udnytter, at managementinterfacet på firewallen er tilgængeligt fra internettet. CFCS anbefaler generelt, at managementinterfaces til firewalls og andre kritiske netkomponenter, ikke er tilgængelige via internettet, samt at disse beskyttes via netværks-segmentering og logisk adgangskontrol.

For Cisco firewalls er der tale om følgende sårbarheder:

- CVE-2016-6366
  Dette er en ny sårbarhed, og Cisco har på endnu ikke udsendt sikkerhedsopdateringer, som imødegår denne sårbarhed. Cisco har dog udsendt workarounds, som imødegår udnyttelsen af sårbarheden.

- CVE-2016-6367
  Cisco har ikke udsendt nogen workaround for denne sårbarhed, men sårbarheden findes kun i Cisco ASA versioner tidligere end version 8.4.

Sårbarhederne gør det muligt for en ondsindet aktør, at udføre Denial of Service angreb mod en Cisco firewall, at få enheden til at reloade, eller mere alvorligt, at overtage kontrollen med firewall'en. Da der er offentliggjort kode, som kan udnytte sårbarhederne, vurderer CFCS, at disse sårbarheder, udgør en alvorlig trussel mod de virksomheder og myndigheder, som benytter sårbare Cisco produkter. CFCS vurderer endvidere, at det er meget sandsynligt, at der er aktører, som vil forsøge at udnytte disse sårbarheder.

Via internettet er det muligt at finde yderligere information om sårbarhederne, hvilke Cisco produkter som er omfattet, samt tilgængelige sikkerhedsopdateringer og workarounds:

http://tools.cisco.com/security/center/viewErp.x?alertId=ERP-56516

Som led i offentliggørelsen af sårbarheder er der endvidere frigivet information om malware, der skaber permanente bagdøre i Cisco firewalls. Cisco har udgivet en vejledning til at identificere evt. tilstedeværelse af uautoriseret software i deres produkter. Vejledningen kan findes via ovenstående link.

CFCS anbefaler, at alle brugere af Cisco firewalls undersøger, om deres produkt er omfattet af sårbarhederne, og i pågældende tilfælde, kontakter deres leverandør, samt følger anbefalingerne fra Cisco. Det anbefales endvidere, at man følger hjemmesiderne fra de øvrige nævnte

producenter af firewalls for at se, om deres produkter er sårbare overfor den offentliggjorte kode, samt følger sikkerhedsanbefalinger, de udsender.

Center for Cybersikkerhed henviser til, at virksomheder og myndigheder kan underrette centeret, såfremt der erkendes angreb relateret til denne trusselsvurdering. Underretningsordningen er beskrevet på centerets hjemmeside.

FE bruger denne skala for sandsynlighed i analyser: