CENTER FOR CYBERSIKKERHED

30. maj 2016
Trusselsvurderingsenheden

Cybervurdering: Truslen fra sårbarhed i Cisco firewalls og routere når disse anvendes som VPN-løsning

Formålet med denne vurdering er at varsle om en alvorlig sårbarhed i Cisco's Adaptive Security Appliance (ASA) software. Sårbarheden er relevant i de tilfælde, hvor Cisco firewalls og routere benyttes som VPN-løsning.

Hovedvurdering

- FE vurderer, at offentliggørelsen af et muligt exploit af sårbarheden betyder, at det er meget sandsynligt, at aktører, for eksempel kriminelle, vil forsøge at udnytte sårbarheden.

- FE vurderer, at den store udbredelse af Cisco's produkter betyder, at aktører vil finde det særligt attraktivt at forsøge at udnytte denne sårbarhed.

- FE vurderer, at den relativt korte tid der er gået mellem Cisco's udsendelse af sikkerhedsopdateringer, og offentliggørelsen af exploit betyder, at mange Cisco enheder med ASA software endnu ikke er opdateret, og derfor stadig er sårbare overfor denne trussel.

- FE anbefaler alle myndigheder og virksomheder med Cisco baserede VPN-løsninger til at undersøge, om deres løsning indeholder potentielt sårbare Cisco enheder, og om nødvendigt implementere de relevante sikkerhedsopdateringer fra Cisco's hjemmeside.

Analyse

Den 10. februar 2016 udgav Cisco et varsel om en sårbarhed i deres Adaptive Security Appliance (ASA) software. Denne software indgår i Cisco routere og firewalls, og benyttes blandt andet ved VPN-løsninger, hvor Cisco produktet fungerer som gateway mellem en virksomheds interne net og internettet. Sårbarheden er således tilgængelig via internettet, hvilket gør den særligt alvorlig.

Sårbarheden er registreret som CVE-2016-1287.

CVSS basis score er 10. Dette betyder, at sårbarheden relativt let kan udnyttes via internettet, og blandt andet kan give en angriber fuld adgang til at læse, slette eller ændre data i det kompromitterede system.

Samtidig med offentliggørelsen af sårbarheden udsendte Cisco sikkerhedsopdateringer, som fjerner sårbarheden. Bemærk at download af sikkerhedsopdateringer fra Cisco's hjemmeside kræver en gyldig licens til det berørte produkt.

Exploit offentliggjort
Den 17. maj 2016 blev der offentliggjort kode som udnytter sårbarheden – et såkaldt exploit. Dette betyder, at kriminelle grupper nu kan udnytte den offentliggjorte kode til at udføre konkrete cyberangreb, hvilket gør sårbarheden mere kritisk.

Mulige konsekvenser af sårbarheden
CFCS har undersøgt koden og kan konstatere, at følgende to angrebsscenarier er mulige:

1. Der kan udføres Denial of Service (DoS) mod berørte Cisco firewalls og routere ved at tvinge Cisco firewall og router til at genstarte konstant. Dette angreb kræver kun meget lidt angrebstrafik modsat traditionelle Distributed DoS angreb, som kræver meget angrebstrafik for at kunne overbelaste adgangen til en server. Konsekvensen af et sådan DoS angreb vil være afbrydelse af eksterne forbindelser til virksomheden via VPN-løsningen, samt afbrydelse af de dataforbindelser, som kontrolleres af den berørte Cisco firewall eller router.

2. Det er muligt at overtage kontrollen af Cisco VPN-server med fulde administrative rettigheder. Derved kan der opnås uautoriseret adgang til virksomhedens netværk. En sådan uautoriseret adgang kan blandet andet udnyttes til at spionere mod myndigheden eller virksomheden, eller til at implementere ondsindet kode i organisationens netværk. Det kunne eksempelvis være med Ransomware, hvor data krypteres, hvorefter dekryptering kun kan ske efter betaling af en løsesum til de kriminelle aktører.

Begge angrebsscenarier kræver, at der anvendes IKEv1 eller IKEv2 VPN-forbindelser. Disse benyttes ved følgende teknologier:

- Site-to-site IPsec VPN.
- Layer 2 Tunneling Protocol (L2TP) over IPsec VPN.
- Remote Access VPN med IPsec VPN-klient.
- IKEv2 AnyConnect.

Sårbarhedens udbredelse
FE vurderer, at den store udbredelse af Cisco's produkter betyder, at det vil være særligt attraktivt for kriminelle aktører at forsøge at udnytte sårbarheden.

Cisco netværksprodukter benyttes i stort omfang i danske myndigheder og virksomheders it infrastruktur, og imødegåelse af sårbarheden er derfor særdeles relevant for mange myndigheders og virksomheders informationssikkerhed.

Følgende Cisco enheder er omfattet af sårbarheden:

- Cisco ASA 5500 Series Adaptive security Appliances.
- Cisco ASA 5500-X Series Next-Generation Firewalls.
- Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers.
- Cisco ASA 1000V Cloud Firewall.
- Cisco Adaptive Security Virtual Appliance.
- Cisco Firepower 9300 ASA Security Module.
- Cisco ISA 3000 Industrial Security Appliance.

Fjernelse af sårbarheden
Cisco udsendte den 10. februar sikkerhedsopdateringer mod denne sårbarhed. Samtidig oplyste Cisco, at der ikke findes nogen såkaldt workaround, som kan mitigere sårbarheden. Eneste mulighed for at fjerne sårbarheden er altså at implementere de relevante sikkerhedsopdateringer eller at deaktivere IKE-baserede VPN-forbindelser.

Der er gået 3 måneder mellem udgivelsen af sikkerhedsopdateringer og udgivelsen af exploit, hvilket betyder, at mange sårbare systemer med stor sandsynlighed endnu ikke er blevet opdateret.

Mange succesfulde cyber angreb skyldes, at sårbare systemer ikke er blevet opdateret med de seneste sikkerhedsopdateringer. FE anbefaler derfor alle berørte myndigheder og virksomheder til snarest muligt at opdatere Cisco enheder, som indeholder den sårbare ASA software.

Detaljer om sikkerhedsopdateringer kan findes på Cisco's hjemmeside

FE bruger denne skala for sandsynlighed i analyser: