CENTER FOR CYBERSIKKERHED

Dato: 23. marts 2017

Trusselsvurdering: Sårbarhed i Cisco-servere kan udnyttes via Telnet

Cisco-servere benyttes i stor udstrækning af myndigheder og virksomheder i Danmark, i særdeleshed indenfor it-sektoren og tele-sektoren. Visse Cisco-servere baseret på IOS software indeholder en sårbarhed, som kan udnyttes via åbne Telnet-forbindelser.

Hovedvurdering

- Det er sandsynligt, at ondsindede aktører vil forsøge at udnytte sårbarheden.
- CFCS anbefaler ejere og administratorer af Cisco-servere, til snarest muligt at undersøge om benyttede servere er sårbare, og snarest muligt at opdatere til en ikke-sårbar version.
- CFCS anbefaler ligeledes alle myndigheder og virksomheder til at sikre, at servere og andet udstyr ikke tillader etablering af en ekstern Telnet-forbindelse.

Analyse

Cisco udgav den 17. marts en Cisco Security Advisory angående en sårbarhed i deres Cisco Cluster Management Protocol (CMP), som er inkluderet i Cisco IOS og IOS XE softwaren.

Sårbarheden gør det muligt for en angriber at genstarte eller eksekvere kode på de berørte servere ved at sende særligt udformede kommandoer via en Telnet-forbindelse. Sårbarheden kan udnyttes via internettet, hvis serveren er konfigureret til at acceptere Telnet-forbindelser fra internettet.

Sårbarheden skyldes en fejl i CMP softwaren, samt at Cisco-serveren benytter Telnet til intern kommunikation mellem servere, som arbejder sammen i et såkaldt cluster. På grund af en fejl er serveren ikke begrænset til kun at acceptere interne Telnet-forbindelser mellem serverne.

Det anbefales ikke at tillade eksterne Telnet-forbindelser til fjernstyring af servere fra internettet. Telnet-protokollen er usikker, blandt andet fordi forbindelsen ikke er krypteret, hvorfor både data og password overføres i klar tekst.

Internettet scannes konstant for servere, som svarer på anmodning om adgang via Telnet, og CFCS ser jævnligt brute-force angreb via internettet på både Telnet- og SSH-forbindelser. Brute-force betyder, at angriberen forsøger at gætte det korrekte password, for derved at skaffe sig fjernadgang til den pågældende server.

Selvom en eventuelt sårbar server ikke er tilgængelig via internettet, så vil denne sårbarhed stadig kunne udnyttes af en aktør, som på anden måde skaffer sig adgang til det interne netværk.

Identificering og fjernelse af sårbarheden
Cisco har udgivet et såkaldt Cisco Security Advisory (cisco-sa-20170317-cmp), som beskriver sårbarheden, hvilke typer servere som er sårbare, samt hvorledes brugeren identificerer, om den benyttede server er sårbar.

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

Den aktuelle Cisco Security Advisory kan findes via dette link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170317-cmp

Anbefaling

CFCS anbefaler alle administratorer og brugere af Cisco-servere til snarest muligt at undersøge, om benyttede servere er sårbare, og i pågældende tilfælde hurtigst muligt at opdatere til en ikke-sårbar version.

CFCS anbefaler ligeledes, at servere og andet udstyr konfigureres til ikke at acceptere eksterne Telnet-forbindelser.

FE bruger denne skala for sandsynlighed i analyser: