CENTER FOR CYBERSIKKERHED

17. april 2018
www.cfcs.dk
CERT-7840

Varsel: Bredt angreb på netværksinfrastrukturer

Til den it-sikkerhedsansvarlige

Center for Cybersikkerhed gør opmærksom på, at de amerikanske og engelske myndigheder i fællesskab har udsendt et varsel, hvori de advarer om APT-aktøres forsøg på at kompromittere netværksenheder såsom routere, switche, firewalls og NIDS'er. De primære mål er ifølge varslet offentlige myndigheder, organisationer fra den private sektor, udbydere af kritisk infrastruktur og ISP'er på verdensplan.

Yderligere information

Angrebene har ifølge varslet blandt andet udnyttet gamle protokoller, dårligt sikrede enheder og EOL-enheder.

En succesfuld kompromittering af eksempelvis en router kan ifølge varslet anvendes til at udføre man-in-the-middle angreb, stjæle intellektuel ejendom, persistere sig i ofrets netværk eller danne grundlag for et fremtidigt angreb.

Varslet kan findes på US-CERT's hjemmeside: https://www.us-cert.gov/ncas/alerts/TA18-106A

Anbefaling

Varslet indeholder uddybende informationer om kampagnen og vejledninger til, hvordan dine systemer kan hærdes overfor en række angrebsvektorer samt en række Indicators of Compromise (IoC'er). Center for Cybersikkerhed anbefaler, at vejledningerne i varslet følges.

Hvis du på baggrund af varslet har mistanke om, at din organisation kan være kompromitteret, kan du kontakte CFCS' vagt via de nedenstående kontaktoplysninger. Observerer du desuden aktiv trafik i din netværkstrafik på baggrund af varsels IoC'er, heriblandt de to nævnte IP-adresser 91.207.57.69 og 176.223.111.160, bør du kontakte CFCS' vagt, før du foretager dig yderligere.

Kontakt
Hvis du har spørgsmål, er du velkommen til at kontakte Center for Cybersikkerheds vagt på telefon 32 89 89 89 eller på mail cert@cert.cfcs.dk.

Om Center for Cybersikkerhed
Center for Cybersikkerhed under Forsvarets Efterretningstjeneste har som hovedopgave at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af.

Denne opgave løses blandt andet ved, at Center for Cybersikkerheds Netsikkerhedstjeneste opdager, analyserer og bidrager til at imødegå avancerede cyberangreb mod myndigheder og virksomheder, der er beskæftiget med samfundsvigtige funktioner.

Om TLP-markeringen

Dette dokument er markeret med Traffic Light Protocol (TLP). Denne markering fortæller dig som modtager, hvordan eller hvorvidt indholdet af dokumentet kan deles ud fra, hvor følsomme informationerne er.
Det er alene Center for Cybersikkerhed som afsender, der kan afgøre dette efter en konkret vurdering af, hvor stor skade en offentliggørelse af informationerne ville medføre. Derfor er det vigtigt, at du som modtager forstår og respekterer den TLP-markering, som vi har angivet.

Definitioner af TLP

TLP-skalaen er opdelt i fire niveauer, som både i navn og farvekode indikerer, hvor følsomme informationerne er, og hvordan de må anvendes af dig som modtager. Det er vigtigt at understrege, at restriktionerne for deling både gælder det markerede dokument samt anden mundtlig og skriftlig omtale af indholdet. Niveauerne er defineret herunder:

- **TLP:RED**
  Informationerne er udelukkende forbeholdt den eller de specifikke modtagere og må ikke deles med andre.
  RED vælges, når afsenderen vurderer, at et misbrug af informationerne eksempelvis kan påvirke en parts privatlivspolitik, omdømme eller operationer.
- **TLP:AMBER**
  Modtageren må, om nødvendigt, dele informationerne internt i sine egne organisationer. AMBER vælges, når afsenderen vurderer, at modtageren er nødt til at involvere andre, herunder organisationsmedlemmer og udvalgte kunder, for at kunne reagere hensigtsmæssigt på indholdet. Dog vurderes indholdet fortsat at kunne påvirke privatlivspolitikker, omdømme og operationer, hvis det deles bredere end disse kredse.
- **TLP:GREEN**
  Modtageren må dele informationerne internt i sine egne organisationer, community eller med samarbejdspartnere inden for sin egen sektor.
  GREEN vælges, når afsenderen vurderer, at indholdet har en bredere relevans i forhold til eksempelvis at skabe awareness på et område. Informationerne er dog stadig følsomme i sådan en grad, at de ikke må deles eller offentliggøres via offentligt tilgængelige kommunikationskanaler og -platforme.
- **TLP:WHITE**
  Informationerne anses ikke som særligt følsomme og kan frit deles.
  WHITE vælges, når afsenderen har vurderet, at der er minimal eller slet ingen risiko ved at offentliggøre informationerne.

Kilde: https://www.first.org/tlp