CENTER FOR CYBERSIKKERHED

Varsel: Kritisk sårbarhed i Apache Log4j kodebibliotek

Til den it-sikkerhedsansvarlige

Center for Cybersikkerhed er blevet bekendt med en sårbarhed i det bredt anvendte Apache Log4j kodebibliotek. Sårbarheden tillader i yderste konsekvens fjernafvikling af arbitrær kode, på bagvedliggende infrastruktur.

Dato: 11. December 2021

Forsvarets Efterretningstjeneste
Att: Center for Cybersikkerhed
Kastellet 30
2100 København Ø

Tlf. 33 32 55 80
E-mail cert@cert.cfcs.dk
www.cfcs.dk

CERT-33300

Yderligere information

Apache Log4j er et bredt anvendt kodebibliotek, der er designet til at forenkle logning, særligt i Java baserede applikationer. Ifølge Apache er der d. 9. december blevet opdaget en kritisk sårbarhed i kodebiblioteket, som kan føre til fjernafvikling af arbitrær kode, såkaldt ”Remote Code Execution”.

Sårbarheden bliver sporet under CVE-2021-44228, og har ifølge Apache en CVSS score på 10.0, dvs. højeste kritikalitet. Sårbarheden bliver også omtalt som ”Log4Shell”.

Flere åbne kilder har rapporteret, at sårbarheden allerede bliver set udnyttet, og forsøgt udnyttet, af ondsindede aktører.

Anbefaling

Center for Cybersikkerhed anbefaler at egenudviklede it-løsninger, der anvender Log4j kodebiblioteket i en udgave mellem version 2.0-beta9 og 2.14.1 opdateres til nyeste version, 2.15.0. I version 2.15.0 er konfigurationen, der muliggør sårbarheden slået fra i bibliotekets standardkonfiguration. Center for Cybersikkerhed anbefaler, at anvendelsen af biblioteket undersøges uanset version.

Hvis det ikke er muligt at opdatere til en nyere version af biblioteket har Apache udgivet en række konfigurationsændringer, der kan forhindre udnyttelsen af sårbarheden. For yderligere information henvises der til Apaches hjemmeside: https://logging.apache.org/log4j/2.x/security.html

Rådgivning
Center for Cybersikkerhed kan i nogle tilfælde bistå med rådgivning om cyber- og informationssikkerhed, herunder styring af informationssikkerhed og risikovurderinger. Center for Cybersikkerheds rådgivning tager som udgangspunkt afsæt i de vejledninger, der kan findes på centerets hjemmeside.

Vejledning
Center for Cybersikkerhed har udarbejdet en række vejledninger om cyber- og informationssikkerhed, herunder "Cyberforsvar der virker", som er en konkret og prioriteret plan til at komme i gang med cyber- og informationssikkerhedsarbejdet. Alle vejledningerne kan findes på centerets hjemmeside og kan frit benyttes.

Kontakt
Hvis du har spørgsmål til ovenstående varsel eller ønsker at høre mere om mulighederne for rådgivning, er du velkommen til at kontakte Center for Cybersikkerhed på telefon 33 32 55 80 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.

Såfremt du som modtager ønsker at videregive oplysninger fra et TLP-markeret dokument til andre end angivet ved markeringen – herunder som led i besvarelse af anmodninger om aktindsigt – anmodes du om forud for evt. videregivelse at indhente en udtalelse fra Center for Cybersikkerhed herom.

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