Information regarding the Log4j2 vulnerability

2021-12-13 - Anish | ESET Nederland - Comments (0) - Security Update

Apache Log4j kwetsbaarheid

Afgelopen vrijdag werd bekend dat er een ernstige kwetsbaarheid is aangetroffen in de veelgebruikte opensource Apache Log4j-tool. De tool, die gebruikt wordt voor het loggen van Java-applicaties, is onderdeel van veel cloud- en enterprise-applicaties. De kwetsbaarheid heeft CVE-identifier CVE-2021-44228 en staat ook bekend als Log4Shell. De kwetsbaarheid die aangetroffen is zorgt ervoor dat criminele groeperingen op afstand code in software uit kunnen voeren met rechten van een bovenliggende applicatie. De bovenliggende applicatie is in dit geval de applicatie die gebruikmaakt van Log4j, waardoor niet in te schatten is welke rechten deze bovenliggende applicatie heeft. Het NCSC heeft de impact mede daarom ingeschaald op hoog en de eerste meldingen van actief misbruik zijn al gezien.

De kwetsbaarheid is bevestigd in Log4j 2.0 t/m 2.14.1. Log4j 1.x is niet onderzocht, deze versie is al sinds 2015 end-of-life en wordt dus niet meer ondersteund door Apache. De kwetsbaarheid is bij updaten naar versie 2.15.0 verholpen.

Wat kun je doen?

Indien jouw organisatie gebruikmaakt van software die draait op Java is de kans aannemelijk dat hier applicaties tussen zitten die de Log4J-tool gebruiken. Het is dan ook belangrijk om te onderzoeken of dit het geval is. Het NCSC heeft een overzicht van kwetsbare software gemaakt die zij doorlopend bijwerken; houd deze pagina de komende periode dus goed in de gaten. Indien hier software tussen staat die gebruikt wordt in jouw organisatie, is het van belang zo spoedig mogelijk te patchen en het advies van het NCSC op te volgen. Daarnaast geeft het NCSC aan op welke Indicators of Compromise je kunt letten.

Lees meer:
https://www.ncsc.nl/actueel/nieuws/2021/december/12/kwetsbare-log4j-applicaties-en-te-nemen-stappen

Daarnaast adviseren wij je om:

- Ervoor te zorgen dat er security-oplossingen geïnstalleerd staan op servers
- Regelmatig te controleren of deze op alle servers nog actief zijn
- Te zorgen dat deze beveiligingsoplossingen op de servers draaien op de laatste versie
- Uitgaand verkeer op servers waar mogelijk te limiteren

ESET-detectie

ESETs Network Attack Protection (IDS) en Web Access Protection-componenten detecteren de Log4j kwetsbaarheid; deze detectie is te herkennen aan de detectienaam JAVA/Exploit.CVE-2021-44228. Deze detectie is beschikbaar voor gebruikers van ESET PROTECT.

Heeft ESET bescherming tegen Log4j?

ESETs Network Attack Protection (IDS) en Web Access Protection-componenten detecteren de Log4j kwetsbaarheid; deze detectie is te herkennen aan de detectienaam JAVA/Exploit.CVE-2021-44228. Deze detectie is beschikbaar voor gebruikers van ESET PROTECT.

Daarnaast zullen alle overige ESET-componenten eventuele "payloads" ook detecteren.

Welke stappen moet ik ondernemen bij klanten die Java gebruiken?

Maken jouw klanten gebruik van Java-applicaties? Bekijk dan welke applicaties van jouw klant kwetsbaar zijn in het overzicht van het NCSC. Dit overzicht wordt doorlopend bijgewerkt, dus moet wel in de gaten worden gehouden. Indien hier software tussen staat die jouw klanten gebruiken is het wenselijk zo spoedig mogelijk te patchen en het advies van het NCSC op te volgen.

Welke stappen moet ik ondernemen bij klanten die Java gebruiken?

Maken jouw klanten gebruik van Java-applicaties? Bekijk dan welke applicaties van jouw klant kwetsbaar zijn in het overzicht van het NCSC. Dit overzicht wordt doorlopend bijgewerkt, dus moet wel in de gaten worden gehouden. Indien hier software tussen staat die jouw klanten gebruiken is het wenselijk zo spoedig mogelijk te patchen en het advies van het NCSC op te volgen.

Maken ESET-oplossingen op de achtergrond gebruik van Log4j?

Op 12 december is geverifieerd en bevestigd dat deze kwetsbaarheid niet van toepassing is op de volgende producten:

- **On-premises products:**
  ESET PROTECT
  ESET Enterprise Inspector
  ESET Antivirus/Internet Security/Smart Security Premium for Windows
  ESET Endpoint Antivirus/Endpoint Security for Windows
  ESET File Security for Windows
  ESET Security for Microsoft SharePoint Server
  ESET Mail Security for Exchange
  ESET Mail Security for Lotus Domino
  ESET Mobile Security for Android
  ESET Parental Control for Android
  ESET HOME - Mobile Apps
  ESET Server Security for Linux
  ESET Security for Kerio
  ESET Endpoint Antivirus for Linux
  ESET Virtualization Security for VMware NSX
  ESET Mail/File/Gateway Security for Linux/BSD v4.5
  ESET NOD32 Antivirus for Linux v4 (Home and Business Edition)
  ESET Endpoint Antivirus for macOS
  ESET Endpoint Security for macOS
  DEM for ConnectWise Automate
  DEM for (Solarwinds) N-able
  DEM for (Solarwinds) RMM
  DEM for NinjaOne
  DEM for Datto
  PSA Plugins

- **Cloud products:**
  ESET PROTECT Cloud
  ESET Enterprise Inspector Cloud
  ESET Cloud Office Security
  RMM for Kasey

- **Encryption products:**
  ESET Endpoint Encryption
  ESET Endpoint Encryption for macOS

ESET Endpoint Encryption Server
ESET Full Disk Encryption
ESET Full Disk Encryption for macOS

- **Portals:**
  ESET Business Accounts
  ESET MSP Administrator
  ESET License Administrator
  ESET HOME

ESET Secure Authentication?
Indien je gebruik maak van "reports" binnen ESET Secure Authentication is de 3rd party applicatie "elasticsearch" wel kwetsbaar en is het advies om deze te updaten.

Bekijk het volgende artikel voor meer informatie:
https://support.eset.com/en/kb8190-vulnerability-log4j2-in-the-reporting-engine-elasticsearch-of-eset-secure-authentication

ESET Statement:
https://support.eset.com/en/alert8188-information-regarding-the-log4j2-vulnerability