Security statement betreffende:

CVE-2021-44228, de log4j 2.x beveiligingskwetsbaarheid

Inleiding
Onlangs hebben meerdere internationale organisaties gebruikers gewaarschuwd voor een kwetsbaarheid in de log4j 2.x-software. Deze kwetsbaarheid kreeg de naam CVE-2021-44228. Details over de kwetsbaarheid zijn gepubliceerd op de NCSC-website: https://www.ncsc.nl/actueel/advisory?id=NCSC-2021-1052. Dit beveiligingslek wordt als kritiek beschouwd omdat het uitvoering van (externe) code mogelijk maakt met zowel opstart-ROOT-autorisaties als gebruikersautorisaties.

Heeft dit invloed op de XiltriX-toepassing?
NEE -> De gebruikersinterface van de Java-client **maakt geen gebruik van Log4j**.
NEE -> De Java-webtoepassing **maakt geen gebruik van log4j**.
NEE -> Apache Tomcat, de servlet-container (webserver) waarop de webtoepassing draait, **gebruikt geen log4j.**

Heeft dit invloed op het Linux besturingssysteem waarop XiltriX is geïnstalleerd?
NEE -> Op de meeste Linux-distributies is log4j 1.x geïnstalleerd als een afhankelijkheid van Apache Tomcat. Merk op dat dit versie 1.x is, **die geen last heeft** van dit beveiligingslek.

Zijn er vergelijkbare kwetsbaarheden gevonden in eerdere versie van log4j?
Er is een verwante CVE-2021-4104 uitgegeven door Apache speciaal voor log4j 1.x, die nog moet worden gepubliceerd. Dit betreft een exploit door een log4j-configuratiebestand aan te passen om het gebruik van een bepaalde logbestand-appender expliciet toe te staan wat het systeem kwetsbaar maakt op dezelfde manier als de CVE voor log4j 2.x. Root-toegang is vereist om dergelijke configuratiewijzigingen aan te brengen, en iemand die root-toegang heeft, hoeft geen misbruik te maken van kwetsbaarheden.

Vragen en aanbevelingen
Mochten er naar aanleiding van dit statement vragen zijn, kunt u altijd contact opnemen met onze support afdeling op support@xiltrix.com. XiltriX International adviseert om de XiltriX applicatie en onderliggende besturingssystemen op regelmatige basis te updaten. Hiervoor levert XiltriX de benodigde support contracten en consultancy.

Met vriendelijke groeten
XiltriX International

Han Weerdesteyn
CCO

Security statement regarding:

CVE-2021-44228, the log4j 2.x security vulnerability

Introduction
Recently multiple international organizations have warned users about a vulnerability in the log4j 2.x software. This vulnerability was named CVE-2021-44228. Details about the vulnerability have been published on the NCSC website: https://www.ncsc.nl/actueel/advisory?id=NCSC-2021-1052. This vulnerability has been deemed critical since it allows for (Remote) code execution with boot ROOT authorizations as well as user authorizations.

Does this affect the XiltriX application?
NO -> The Java client UI **does not use Log4j**.
NO -> The Java web application **does not use log4j**.
NO -> Apache Tomcat, the servlet container (webserver) running the web application, **does not use log4j**.

Does this affect the Linux OS on which XiltriX is installed?
NO -> On most Linux distributions log4j 1.x is installed as a dependency of Apache Tomcat. Note that this is version 1.x, which **does not suffer** from this security vulnerability.

Were similar vulnerabilities found in earlier versions of log4j?
There is a related CVE-2021-4104 issued by Apache specifically for log4j 1.x, which has yet to be published. This concerns an exploit by modifying a log4j configuration file to explicitly allow the use of a certain log file appender which makes the system vulnerable in the same way as the CVE for log4j 2.x. Root access is required to make such configuration changes, and one who has root access does not need to exploit vulnerabilities.

Questions and recommendations
If there are any questions regarding this statement, you can always contact our support department at support@xiltrix.com. XiltriX International advises to update the XiltriX application and underlying Operating Systems on a regular basis. For this, XiltriX provides the necessary support contracts and consultancy.

With best regards
XiltriX International

Han Weerdesteyn
CCO