21 dec 2021 -09:10

Het Centrum voor Cybersecurity België verwacht grote problemen bij bedrijven en organisaties die geen actie ondernemen tegen Log4j kwetsbaarheid

Bedrijven die Apache Log4j software gebruiken en nog geen acties ondernamen, kunnen de komende dagen en weken grote problemen verwachten. Deze kwetsbaarheid wordt actief uitgebuit door cybercriminelen. Wie geen actie onderneemt, kan nu zeer snel het slachtoffer worden van een cyberaanval.

Afgelopen week werd een kwetsbaarheid ontdekt in Apache Log4j. Dit is software die veel gebruikt wordt in webapplicaties en allerlei andere systemen. De kwetsbaarheid maakt het voor aanvallers mogelijk de rechten van webservers op afstand te misbruiken. Omdat deze software zo wijd verspreid is, valt het moeilijk in te schatten hoe de ontdekte kwetsbaarheid zal geëxploiteerd worden en op welke schaal. Cybercriminelen proberen intussen de kwetsbaarheid uit te buiten en zoeken actief naar kwetsbare systemen. Het spreekt voor zich dat dit een gevaarlijke situatie is. Er zijn updates beschikbaar.

Het Centrum voor Cybersecurity België (CCB) raadt gebruikers van Apache Log4j dan ook aan om zo snel mogelijk de beschikbare updates te installeren. Lees het techische advies hier. Bent u niet zeker of er binnen uw organisatie gebruik wordt gemaakt van Apache Log4j, vraag dit dan na bij uw softwareleverancier.

Het CCB monitort de situatie nauwgezet en zal nieuwe informatie over updates publiceren zodra die beschikbaar is.

Bedrijven en organisaties die slachtoffer worden van een cyberaanval kunnen dit melden bij cert@cert.be.

Centrum voor Cyber Security België
Wetstraat 18
1000 Brussel
België
http://www.ccb.belgium.be

Katrien - Eggers
Communicatieverantwoordelijke CCB
+32 485 76 53 36
katrien.eggers@cert.be