COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

Ministerie van Volksgezondheid, Welzijn en Sport

L.s.,

Hierbij informeren wij u over een ernstige kwetsbaarheid in een veelgebruikt stuk computersoftware Apache Log4j. Wij doen hierbij een dringende oproep aan u als koepelorganisatie om uw leden te informeren over deze kwetsbaarheid en hen te adviseren hier actie op te ondernemen.

In de computersoftware Apache Log4j zit een ernstige fout. Apache Log4j wordt gebruikt in heel veel software en applicaties zonder dat u dat merkt. Hoogstwaarschijnlijk maken ook veel computersystemen van zorginstellingen en zorgaanbieders gebruik van deze software. Het is van groot belang dat de fout zo snel mogelijk wordt opgelost voordat criminelen massaal misbruik maken van dit lek, bijvoorbeeld door gijzelsoftware ongemerkt naar binnen te loodsen.

Via deze fout kunnen cybercriminelen en hackers zich simpel toegang verschaffen tot netwerken en (medische) gegevens. Dit kan grote gevolgen hebben, ook voor systemen bij zorginstellingen. De kwetsbaarheid is ook aangetroffen bij zorginstellingen die NEN7510 gecertificeerd zijn en reeds beveiligingsmaatregelen tegen digitale inbraak hebben getroffen. Vorige week vrijdag sloegen cybersecurityspecialisten wereldwijd groot alarm. Met man en macht proberen cybersecurityspecialisten te voorkomen dat criminelen misbruik maken van deze fout. Daar hebben we ook de zorginstellingen zelf bij nodig. Men kan het volgende doen:

Advies:

- Scan alle systemen op de aanwezigheid van Apache Log4j.
- Installeer zo snel mogelijk de beschikbare updates, en houd deze bij.
- Onderzoek of de kwetsbare systemen reeds zijn misbruikt.
- Zorg dat u bent voorbereid op een mogelijke digitale aanval.

Niet alleen de zorgsector maar heel Nederland heeft te maken met deze digitale crisis. Het Nationaal Cyber Security Centrum geeft op haar website (www.ncsc.nl) uitleg over deze digitale dreiging. Ook heeft het NCSC een online overzicht gemaakt met systemen die gebruikmaken van Apache Log4j. Hier kunt u controleren of programma's of apparaten die u gebruikt kwetsbaar zijn. U vindt het overzicht via onze liveblog of op de website van het NCSC.

Op de website van Z-CERT (www.z-cert.nl), het expertisecentrum voor cybersecurity in de zorg, staat een liveblog over Apache Log4j. Volg deze pagina voor meer informatie.

Bij vragen over de Apache Log4j kwetsbaarheid adviseren wij zorginstellingen om contact op te nemen met hun systeembeheerder of leverancier. Dit bericht is in samenwerking met het ministerie van Volksgezondheid, Welzijn en Sport opgesteld.

Met vriendelijke groet,
Team Z-CERT

Stichting Z-CERT
Stationsplein 121
3818 LE Amersfoort
+31 (0)33 737 06 09
info@z-cert.nl
www.z-cert.nl
KvK 67374972