21 Dec 2021 -09:10

The Centre for Cybersecurity Belgium expects major problems for companies and organisations that do not take action against Log4j vulnerability

Companies that use Apache Log4j software and have not yet taken action can expect major problems in the coming days and weeks. This vulnerability is being actively exploited by cybercriminals. Those who do not take action can now very quickly become the victim of a cyber-attack.

Last week a vulnerability was discovered in Apache Log4j. This is software that is often used in web applications and all kinds of other systems. The vulnerability makes it possible for attackers to abuse the rights of remote web servers. Because this software is so widely distributed, it is difficult to estimate how the discovered vulnerability will be exploited and on what scale. Meanwhile, cybercriminals are trying to exploit the vulnerability and are actively looking for vulnerable systems. It goes without saying that this is a dangerous situation. Updates are available.

The Centre for Cybersecurity Belgium (CCB) therefore advises users of Apache Log4j to install the available updates as quickly as possible. Please follow this technical advise. If you are not sure whether Apache Log4j is used within your organisation, ask your software supplier.

The CCB is monitoring the situation closely and will publish new information on updates as soon as it becomes available.

Companies and organisations that become the victim of a cyber-attack can report this to cert@cert.be.

Centre for Cyber Security Belgium
Rue de la Loi 18
1000 Brussels
Belgium
http://www.ccb.belgium.be

Katrien - Eggers
Communications officer
+32 485 76 53 36
katrien.eggers@cert.be