Java library Log4j

Immediate action required due to vulnerability in Java library Log4j

13.12.2021

The Log4j software library used in countless JAVA applications is affected by a critical vulnerability. IT systems and services using the software library are already being actively exploited over the Internet. The Hessian Commissioner for Data Protection and Freedom of Information (HBDI) provides information about the urgent need for action.

Fotolia_103397196_S.jpg

© Weissblick fotolia.com

The Hessian Commissioner for Data Protection and Freedom of Information (HBDI) informs about the urgent need for action regarding the vulnerability in the Java library Log4j (Log4j).

Due to a cyber security warning of the red warning level from the Federal Office for Information Security (BSI), the HBDI for its part informs about the vulnerability in Log4j (CVE-2021-44228) because of its great scope and criticality. The IT threat situation is particularly high because a large number of IT systems are affected and because the Log4Shell vulnerability can be exploited via the Internet with little technical effort. After the worldwide mass scans observed by the BSI at the weekend, information about successful compromises is now also available. It can be expected that attackers' activities using the vulnerability will increase significantly in the next few days and the risk of compromise is very high.

This means that the responsible bodies must assume a real, immediate and significant threat to the systems and services affected, so that there is an urgent need for action. Due to the large number of affected software products, IT systems and services known to date, there is an acute risk of breaching the protection of personal data processed using them.

If there is a vulnerability in Log4j, the security of the processing in accordance with Art. 32 GDPR for the affected systems and possibly beyond is no longer fully guaranteed. It is the responsibility of those responsible to restore the security of the processing. Accordingly, the HBDI strongly recommends that

Those responsible find out about the vulnerability, identify affected IT systems and services and take the necessary measures, order processors to take action of their own accord, take appropriate measures and approach the responsible persons concerned,

Manufacturers check their products for the existence of the vulnerability, actively inform affected customers, develop and make available recommendations for action, and develop and provide updates, patches or similar to fix the vulnerability.

Closing the vulnerability is not sufficient here. Those responsible must also check whether there have already been successful attacks. In this case, further measures must be taken and it must be checked whether violations of the protection of personal data must be reported to the HBDI in accordance with Art. 33 DS-GVO.

Log4j is a helper component used in many Java applications worldwide. It is used by the affected applications for event logging (logging). Log4j is not only used in independently developed and operated company applications, but is also an integral part of a large number of software products and IT devices from different manufacturers and service providers. Due to the purpose of logging, Log4j can also be used as a sub-component that is not immediately recognizable.

Current information and recommendations for action on the Log4j vulnerability can be found in the cyber security warning from the BSI.

Left: Federal Office for Information Security; Critical vulnerability in log4j Java library

Contact for press representativesPress spokeswoman: Ms. Maria Christina RostPress and public relations: Telephone: +49 611 1408 119The Hessian Commissioner for Data Protection and Freedom of InformationP.O. Box 316365021 Wiesbaden

PrintSend as email