Dallmeier

Security Advisory Log4Shell

Log4Shell (CVE-2021-44228) is a zero-day arbitrary code execution vulnerability in the popular Java logging framework Log4j. The vulnerability was privately reported to Apache by Alibaba's Cloud Security Team on November 24, 2021 and publicly disclosed on December 9, 2021. The vulnerability takes advantage of Log4j's failure to validate LDAP and JNDI requests, allowing attackers to execute arbitrary Java code on a server or another machine.

In addition to this advisory, note the numerous publications about Log4Shell on the Internet, such as a (non-exhaustive) publication of affected services in a github project. Please also pay attention to corresponding reports of the Bundesamt für Sicherheit in der Informationstechnik (BSI) or of the National Institute of Standard and Technology (NIST).

No Endangerment

Dallmeier has already reviewed all recording systems, cameras as well as software products regarding the Log4Shell vulnerability. The **Log4j** framework is **not used** in the following products. These products are **not at risk** from exploitation of the Log4Shell vulnerability.

- All network cameras
- All recording systems
- Panomera® Streaming Server
- CAT Server
- External AI Server
- SeMSy® Compact
- SMAVIA Viewing Client
- PService3
- Dallmeier Device Manager
- DMVC Apps (iOS, Android)
- SeMSy® III Video Management System

Endangerment

Dallmeier experts have identified **one vulnerability** in the logging platform of the **HEMISPHERE® High Availability** solution. Patches and updates are available for the underlying open source software. These will be compiled in a comprehensive **infrastructure update** in a timely manner.

Procedure

Dallmeier experts have already developed an **immediately available solution to fix the vulnerability** in the HEMISPHERE® High Availability solution. By **adjusting the configuration** of relevant system components, the **exploitation of the Log4Shell vulnerability can be prevented**. These adjustments can be made remotely during operation.

The HEMISPHERE® High Availability solution is exclusively **used in projects** that are **directly supported by Dallmeier experts**. The corresponding contact persons of the **project teams will proactively approach affected customers and partners** and **coordinate the implementation of the adjustments**. In addition, they will be available for any inquiries, just like the contact persons of the sales teams.

General Endangerment

Note that **due to the wide distribution** of the Java logging framework Log4j, a large number of devices and applications are at risk for the Log4Shell vulnerability. Apart from Dallmeier components, **all other components of a video system** are thus potentially at risk, such as:

- Servers
- Routers and switches
- Virtual systems
- 3rd party network cameras

Dallmeier products and third-party products purchased through Dallmeier are always delivered with the latest updates and security patches at the time of shipment.

At present, corresponding updates and patches are already offered. If necessary, note the current information from the relevant manufacturers.

V1.0.0 2021-12-14 Specifications subject to change without notice. Errors and misprints excepted.