VidiView R4 – Security Bulletin – Log4j vulnerability

Lund 2021-12-14

Distributed Medical AB, Filip Strandqvist

This letter contains important information about your VidiView Server installation. The intended audience for this letter is technical personal in charge of system management and maintenance.

At this time, you may be aware of the found vulnerability in the commonly used Java library **log4j**. The vulnerability is also commonly referred to as CVE-2021-44228. Please read more about this at https://nvd.nist.gov/vuln/detail/CVE-2021-44228

From a development perspective the log4j library exists in a .net-encapsulated form (embedded into a .dll). The functionality within the VidiView Server using this library is related to Dicom export and import and we have used our best efforts to try and investigate the inner workings of this library in relation to our application. We have not been able to expose any kind of vulnerability in our use case. Hence – no need to any action on the account of VidiView.

No other part of the VidiView products contain the log4j library.

For full technical transparency we like to clarify;

- **We use version 1.2 of the log4j library. The mechanism that is used for the exploit was introduced in version 2.0.**
- The exploit requires full internet connection from the vulnerable host (the VidiView server)
- The exploit requires a JRE on the host (to execute the code downloaded from the malicious host on the internet). **A JRE is not a requirement for a VidiView server and should never be installed on a VidiView server host!**
- In most use cases only Dicom export is used with the VidiView Server and no incoming calls to the Dicom-library is accepted – whereas the vulnerability is not exposed.
- If Dicom receive (StoreSCP) is configured, incoming calls to the Dicom-library will be accepted. In this scenario logging of such incoming calls will be logged, not by log4j, but rather with our own logging-module which is instantiated on logging calls (*based on our source code review performed 2021-12-13*) on all occasions.

An easy-to-understand description of the vulnerability can be found here
https://www.govcert.ch/blog/zero-day-exploit-targeting-popular-java-library-log4j/

You VidiView Server-installation reside on IT-infrastructure supplied by the end-user organization and falls out-of-scope with this bulletin. It is, however, equally important to make sure this infrastructure safe, updated and properly secured from a network perspective to protect oneself from this type of exploit.

If you have questions regarding this bulletin, you may consult us at any time!

Distributed Medical

Ideon Researchpark, Beta 1
S-223 70 Lund
Sweden

Tel +46-755-55 1200
http://www.distributedmedical.com
info@distributedmedical.com