“Apache Log4j” vulnerabilities Statement

Publication date: 2021 December 21

Update A: 2021 December 22
Update B: 2021 December 23
Update C: 2021 December 28
Update D: 2022 January 13
Update E: 2022 June 09

This document aims to provide information on the assessment of a potential product impact linked with the recently disclosed set of vulnerabilities affecting “Apache Log4j”.

Executive Summary

As detailed in the CISA cybersecurity advisory AA21-356A, three vulnerabilities CVE-2021-44228 (known as “Log4Shell”), CVE-2021-45046, and CVE-2021-45105 have been found on Apache Log4j. The CVE-2021-44228 shows an overall CVSS score of 10.0 which is the highest CVSS score and is considered critical.

Vulnerabilities concern multiple OT and IT systems and products.

CVE-2021-44228 and CVE-2021-45046 were rated as critical vulnerabilities by Apache. They are considered severe due to their broad usage in IT and OT products and their easy exploit. According to AA21-356A “Log4Shell is especially critical because it allows malicious actors to remotely run code on vulnerable networks and take full control of systems”. Applying mitigations, even if resource intensive, is strongly recommended.

Vulnerabilities are the following: Improper Neutralization of Special Elements used in an Expression Language Statement, Improper Input Validation, Deserialization of Untrusted Data, Uncontrolled Resource Consumption and Uncontrolled Recursion.

The segments of the Fresenius group are actively monitoring the disclosed “Apache Log4j” vulnerabilities and analysis actions were taken to determine if any impact on our current products.

Fresenius products assessment

- The following list of products were assessed and are **affected** by Apache Log4j.

Fresenius Medical Care

Product	**Versions**
Infrastructure Data Management Systems (IDMS)	DataCOM Gateway with ESF Version 6.x
Home Bridge	DataCOM Gateway with ESF Version 6.x
Remote Service	DataCOM Gateway with ESF Version 6.x

- The following list of products were assessed and are **not affected** by Apache Log4j.

Fresenius Medical Care

Product	Versions
5008	All versions
5008S	All versions
6008	All versions
Silencia	All versions
SleepSafe Harmony	All versions
Infrastructure Data Management Systems (IDMS)	DataCOM Gateway with ESF Version 5 or below
Home Bridge	DataCOM Gateway with ESF Version 5 or below
Remote Service	DataCOM Gateway with ESF Version 5 or below

Update A

Product	Versions
7Connect	All versions
communicationDataLink (cDL)	All versions
multiConnectIT	All versions
theHub (CAPD project)	All versions
theHub (Matterhorn project)	All versions
theHub (Order Processing management project)	All versions
theHub (Portable project and Sunstone project)	All versions
uniDataLink (UDL)	All versions

Update B

Product	Versions
Therapy Monitor (TMon), excl. plug-in #400	All versions
Therapy Support Suite (TSS)	All versions
PatientOnLine (POL)	All versions
Fluid Management Tool (FMT)	All versions
Anaemia Control Model (ACM)	All versions

Update D

Product	Versions
MFTPro	All versions
mCM (HL7 Converter)	All versions
MFTClassic	All versions
Genius 90	All versions

Update E

Product	Versions
BCM – Body Composition Monitor	All versions

Fresenius Kabi

Update B

Product	Versions
Infusion Pumps – Agilia (Agilia Intuitive Generation and Agilia Connect)	All versions
Infusion Pumps – Exelia	All versions
Infusion Pumps – Orchestra	All versions
Enteral Nutrition Pumps – Amika	All versions
Infusion Pumps – INfusia	All versions
Enteral Nutrition Pumps – Enfusia	All versions
Monitoring Devices – Conox	All versions
Vigilant Software Suite	All versions
Agilia Partner	All versions
Exelia Partner	All versions
Amika Partner	All versions
INfusia Centro	All versions

Update C

Product	Versions

Apache Log4j vulnerabilities impact rationale

None of “Apache Log4j” reported vulnerabilities can be exploited on these products.

The following vulnerabilities are associated with the “Apache Log4j” cybersecurity advisory:

- CVE-2021-44228
- CVE-2021-45046
- CVE-2021-45105

General Cybersecurity recommendations

Proper cybersecurity hygiene and behavior is required to safely integrate Medical Devices into IT infrastructure. The Fresenius Group recommends operators of Medical Devices and software to incorporate the following industry best practices into their defense-in-depth strategy:

- Conduct a comprehensive and periodic security risk assessment on the medical network in accordance with operational security best practices such as ISO 27002
- Minimize network exposure for all medical devices and systems, and ensure that they are not accessible from the Internet
- Locate Fresenius Medical Devices behind firewalls, in dedicated medical networks, isolated from all other IT networks
- Monitor and control access and traffic to the dedicated medical network
- Implement application firewalls capable of deep packet inspection to help protect against zero-day vulnerabilities and the latest exploits
- Use appropriate authentication and authorization of users on the network
- Implement physical controls that ensure no unauthorized persons would have access to the medical devices and systems
- Ensure that all programming software and equipment (service laptops, etc.) are kept in locked cabinets and are never connected to any network other than the medical network they are intended to service
- Ensure that all portable media used for data exchange with the medical network (such as CDs, USB drives, etc.) are scanned before use
- Implement a process to monitor, prevent and contain malwares and computer viruses.

Institutionalizing strong cybersecurity policies and following the industry best practices relative to IT security could minimize exposure to threats. These threats may include but not limited to: Data Leak, Data Corruption, Data Loss, Network or Service Outage, etc.

References

Regarding “Apache Log4j” vulnerabilities more details can be found on:

Apache Log4j Security Vulnerabilities: Apache website
CISA Cybersecurity Advisory: AA21-356A
JCDC guidance: Apache Log4j Vulnerability Guidance

Contacts

For any questions or suggestions please contact your regional marketing manager.