

Document ID	Revision	Date	Initial Publication	Document category
AAGS-HOSP-SA-2021-001	3	2021-12-21	2021-12-14	Security Advisory

TLP:WHITE

No Restriction on Distribution

AAGS-HOSP-SA-2021-001

SEVERITY: INFORMATIONAL

OVERVIEW

ASSA ABLOY Global Solutions Hospitality has investigated several vulnerabilities (*CVE-2021-44228*, *CVE-2021-4104*, *CVE-2021-17571*, *CVE-2021-45046*, *CVE-2021-45105*, *CVE-2021-42550*) related to the commonly used Java logging utility Apache Log4j and Logback. This investigation followed our Product Security Incident Response (PSIR) Policy to identify affected products, assessing any potential implications for our customers, determine what mitigation steps should be taken, and notify affected customers.

We have not found that the vulnerabilities impacts our products.

While our product investigation is done, we will continue to monitor the threat environment and update this advisory if this situation changes. Our security teams are actively monitoring our environments and updated our defense-in-depth tools.

ADDITIONAL INFORMATION:

While Visionline isn't vulnerable to these CVE's, it is indirectly using Log4J1 in a connected service. Visionline is not using the prerequisites to be able to perform an exploit of CVE-2021-4104 and CVE-2021-17571. For Visionline customers who still would like to remove Log4J1 in their installation, it is possible to remove it entirely as a short-term solution. We have created a guide for you available at our Service Portal on this topic.

CONTACT INFORMATION

If you have any questions about this advisory, don't hesitate to contact our 24/7 support on +1 214-833-6778.

Service Portal: <https://my.assaabloyglobalsolutions.com/assaabloy>

REFERENCES

CVE-2021-44228: <https://nvd.nist.gov/vuln/detail/CVE-2021-44228>

CVE-2021-4104: <https://nvd.nist.gov/vuln/detail/CVE-2021-4104>

CVE-2021-17571: <https://nvd.nist.gov/vuln/detail/CVE-2019-17571>

CVE-2021-45046: <https://nvd.nist.gov/vuln/detail/CVE-2021-45046>

CVE-2021-45105: <https://nvd.nist.gov/vuln/detail/CVE-2021-45105>

Document ID	Revision	Date	Initial Publication	Document category
AAGS-HOSP-SA-2021-001	3	2021-12-21	2021-12-14	Security Advisory

CVE-2021-42550: <https://nvd.nist.gov/vuln/detail/CVE-2021-42550>

Apache's Disclosure: <https://logging.apache.org/log4j/2.x/security.html>

TERMS OF USE

THIS DOCUMENT IS PROVIDED "AS IS". IT DOES NOT IMPLY ANY KIND OF GUARANTEE, WARRANTY, OR UNDERTAKING, NOR DOES IT EXPAND THE SCOPE OF ANY GUARANTEE, WARRANTY OR UNDERTAKING MADE IN ANY AGREEMENT TO WHICH AN ASSA ABLOY GROUP COMPANY IS A PARTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. ANY USE OF THE INFORMATION CONTAINED HEREIN OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK. ASSA ABLOY GLOBAL SOLUTIONS RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A STANDALONE COPY OR PARAPHRASE OF THE TEXT OF THIS DOCUMENT THAT OMITTS THE DISTRIBUTION URL IS AN UNCONTROLLED COPY. UNCONTROLLED COPIES MAY LACK IMPORTANT INFORMATION OR CONTAIN FACTUAL ERRORS. THE INFORMATION IN THIS DOCUMENT IS INTENDED SOLY FOR END USERS' LAWFUL USE OF ASSA ABLOY GLOBAL SOLUTIONS PRODUCTS.