Product Security Advisory
19/10/2022

Apache Common Text (ABLOY-PSA-2022-003)

TLP: WHITE
Disclosure is not limited.

Rating: Low

OVERVIEW

On the 18th of October the National Cyber Security Centre of Finland published an alert about a critical vulnerability found in Apache Common Text module. Apache Commons Text performs variable interpolation, allowing properties to be dynamically evaluated and expanded.

Abloy immediately launched an investigation on the possible impacts of this vulnerability and the required recommended actions to restrict harmful impacts to our customers. Investigating and limiting the impacts of this vulnerability have been our top priority from the start.

SCOPE LIMITATION

This Product Security Advisory is only applicable for ABLOY Customer Products and Services. Some products although distributed by Abloy will be the responsibility of the original manufacturer or by ASSA ABLOY group or its subsidiaries. This does also not apply to Abloy internal IT systems and Data processing systems. Abloy can still be contacted as a re-seller for any products sold by Abloy if you have questions.

ADVISORY STATUS

Investigation Ongoing. Abloy continues investigating this issue, as of now you can see the current status for ABLOY Customer Products and Services in the following tables.

AFFECTED PRODUCTS (see Remediation/Mitigation section for actions)

Product	Version
ABLOY OS	2.8 – 2.13.x

PRODUCTS UNDER INVESTIGATION

Product	Version
ABLOY CORE	All versions
ABLOY PULSE /ACCENTRA	All versions
ABLOY FLEXIM	v. 3-6
My Abloy	All versions

Product Security Advisory
19/10/2022

Apache Common Text (ABLOY-PSA-2022-003)

PRODUCTS THAT ARE NOT AFFECTED

Product	Version
ABLOY CUMULUS	All versions
FLEXIM PRO /COMPACT	All versions
ABLOY OS (Safea)	<2.8

VULNERABILITY DESCRIPTION

The risk of malpractice of the software products affected is extremely limited and estimated as **LOW.**

Impact

After careful investigation the affected module is used by some of ABLOY products, but not in such a way to be vulnerable.

Severity

The issue is classified as important by the Apache community, and it has further been given a CVSS v3.1 score of 9.8 (Critical). Our assessment is that it is an overall risk score of **LOW** for how it is used in affected ABLOY products.

Remediation/ Mitigation

The recommended mitigation by Apache community is to patch the component in question to latest version 1.10.0. Abloy has incorporated this dependency into our code. Patching updates will be published with the next version releases (according to the normal schedule), and we recommend that you update to latest version according to normal plans.

ABLOY OS 2.7 – 2.13.x
Fix is being worked into next major release, version 2.14, coming soon.

CONTACT INFORMATION

For further information, please do not hesitate to get in touch with us:

- Product Security Center
  - product.security@abloy.com or
  - +358 10 346 5010 (EET 8-16 during Finnish Business Days)

REFERENCES

https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_19/2022 (in Finnish)
https://nvd.nist.gov/vuln/detail/CVE-2022-42889.

Product Security Advisory
19/10/2022

Apache Common Text (ABLOY-PSA-2022-003)

REVISION HISTORY

Revision	Date	Description
1.0	19/10/2022	The initial publication of the advisory

TERMS OF USE