10 years CERT-EU

Security Advisory 2022-005

Critical Vulnerability in Ivanti Products

January 19, 2022 — v1.0

TLP:WHITE

History:

- *19/01/2022 — v1.0 – Initial publication*

Summary

On January 17th, Ivanti updated its advisory related to `CVE-2021-44228` vulnerability affecting some of its products. While this CVE affects the Java logging library `log4j` [1], all products using this library are vulnerable to Unauthenticated Remote Code Execution.

Technical Details

The vulnerability exists in the Java logging library `log4j`. An unauthenticated remote attacker might exploit this vulnerability by sending specially crafted content to the application to execute malicious code on the server [1].

Affected products

Product	affected versions	Mitigation / Fix
Avalanche	6.3.0, 6.3.1, 6.3.2, and 6.3.3	Available [3]
Ivanti File Director	2020.3, 2021.1, 2021.3	Available [4]
MobileIron	See [5]	Available [5]

Recommendations

Ivanti and CERT-EU strongly recommends to apply mitigations or fixes mentioned in the Affected Products section.

References

[1] https://media.cert.europa.eu/static/SecurityAdvisories/2021/CERT-EU-SA2021-067.pdf

[2] https://forums.ivanti.com/s/article/CVE-2021-44228-Java-logging-library-log4j-Ivanti-Products-Impact-Mapping?language=en_US

[3] https://forums.ivanti.com/s/article/CVE-2021-44228-Avalanche-Remote-code-injection-Log4j?language=en_US

[4] https://forums.ivanti.com/s/article/Apache-Log4j-Zero-Day-Vulnerability-and-Ivanti-File-Director-CVE-2021-44228?language=en_US

[5] https://media.cert.europa.eu/static/SecurityAdvisories/2021/CERT-EU-SA2021-070.pdf