CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-072

ArcGIS Critical Vulnerability

December 16, 2021 — v1.0

TLP:WHITE

History:

- *16/12/2021 — v1.0 – Initial publication*

Summary

On December 16th, Esri updated its blog post related to CVE-2021-44228 affecting ArcGIS products, especially ArcGIS Enterprise and ArcGIS Server [1]. While this CVE affects the Java logging library `log4j`, all products using this library are vulnerable to Unauthenticated Remote Code Execution [2].

ArcGIS Enterprise components contain the vulnerable log4j library. However, Esri specifies in its blog post that there is no known exploit available for any version of a base ArcGIS Enterprise deployment or stand-alone ArcGIS Server at this time. Still, ESRI released a Log4Shell mitigation scripts that fully address CVE-2021-44228.

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 [2].

Affected products

All versions of ArcGIS Enterprise and ArcGIS Server are vulnerable.

Notes:

- ArcGIS Monitor does not contain Log4j library, therefore, it is not vulnerable.
- ArcGIS Pro contains log4j library but the vulnerability cannot be exploited since the software does not listen for remote traffic.

Recommendations

Esri recommends to apply the mitigation script to all installations of ArcGIS Enterprise and ArcGIS Server of any version of the software as soon as possible. Note that the mitigation script only removes the vulnerable `JndiLookup` class, thereby the vulnerable log4j library version will still be present on the systems.

The instructions to run the mitigation script according to the products can be found here:

- ArcGIS Server: https://support.esri.com/Technical-Article/000026951
- Portal for ArcGIS: https://support.esri.com/Technical-Article/000026950
- ArcGIS Data Store: https://support.esri.com/Technical-Article/000026949
- ArcGIS GeoEvent Server: https://support.esri.com/Technical-Article/000026956

References

[1] https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-software-and-cve-2021-44228-aka-log4shell-aka-logjam/

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