CERT-EU

Security Advisory 2022-028

Apache Struts RCE Vulnerability

April 20, 2022 — v1.0

TLP:WHITE

History:

- *20/04/2022 — v1.0 – Initial publication*

Summary

The Apache Software Foundation has released a security advisory about a possible remote code execution vulnerability CVE-2021-31805 in the Apache Struts web application framework [1]. This vulnerability was previously addressed with CVE-2020-17530 but the fix was incomplete [2].

Technical Details

Apache Struts is a widely used open-source framework for developing web applications in the Java programming language. The vulnerability CVE-2021-31805 is based on the forced OGNL evaluation. Some of the tag's attributes could perform a double evaluation if a developer applied forced OGNL evaluation by using the `%{...}` syntax. Using forced OGNL evaluation on untrusted user input can lead to a remote code execution and security degradation.

Products Affected

The Apache Software Foundation announced that Struts versions 2.0.0 to 2.5.29 are affected.

Recommendations

Upgrade to Apache Struts version 2.5.30 or greater.

Workarounds

It is recommended to avoid using forced OGNL evaluation in the tag's attributes based on untrusted/unvalidated user input. Apache Sofrware Foundation has published Security Guide for further recommendations [3].

References

[1] https://cwiki.apache.org/confluence/display/WW/S2-062

[2] https://cwiki.apache.org/confluence/display/WW/S2-061

[3] https://struts.apache.org/security/#do-not-use-incoming-untrusted-user-input-in-forced-expression-evaluation