CERT-EU Security Advisory 2018-022

Apache Struts – Critical Remote Code Execution Vulnerability

August 23, 2018 — v1.0

History:

- *23/08/2018 — v1.0: Initial publication*

Summary

Semmle researchers discovered and disclosed a critical remote code execution vulnerability (CVE-2018-11776) in the Apache Struts web application framework [1, 2]. That flaw could allow remote attackers to run malicious code on the affected servers.

Technical Details

Apache Struts is a widely used open source framework for developing web applications in the Java programming language. This vulnerability is caused by insufficient validation of user-provided inputs in the core of the Struts framework. The vulnerability is present in the servers that meet specific configuration requirements:

1. The `alwaysSelectFullNamespace` flag is set to true in the Struts configuration (this is done automatically in the case of usage of the popular Struts Convention plugin).
2. The application uses actions that are configured without specifying a namespace, or with a wildcard namespace. This applies to actions and namespaces specified in the Struts configuration file, but also to actions and namespaces specified in Java code if the Struts Convention plugin is in use [2].

Products Affected

The Apache Software Foundation announced that Struts versions 2.3 to 2.3.34 and 2.5 to 2.5.16 are affected. Unsupported versions of the framework might be also affected.

Recommendations

Upgrade to Apache Struts version 2.3.35 or 2.5.17.

Workarounds

Verify that you have set namespace (if applicable) for all defined results in underlying configurations. Also verify that you have set value or action for all url tags in your JSPs. Both are needed only when their upper action(s) configurations have no or wildcard namespace.

Note: This is a temporal workaround. The solution is to upgrade to Apache Struts version 2.3.35 or 2.5.17 ASAP because they also contain critical overall proactive security improvements. Moreover, accordingly to the researcher, even if an application is currently not vulnerable, *an inadvertent change to a Struts configuration file may render the application vulnerable in the future.* It is therefore strongly advised to upgrade Struts components [1, 3].

Exploits

The exploit can be triggered just by visiting a specially crafted URL on the affected web server, allowing attackers to execute malicious code and eventually take complete control over the targeted server running the vulnerable application [4].

References

[1] https://semmle.com/news/apache-struts-CVE-2018-11776

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-11776

[3] https://cwiki.apache.org/confluence/display/WW/S2-057

[4] https://thehackernews.com/2018/08/apache-struts-vulnerability.html