computer emergency response team CERT-EU for the EU institutions, bodies and agencies

CERT-EU Security Advisory 2017-005

Critical Apache Struts 2 Framework Vulnerability

March 9, 2017 — v1.0

History:

- *09/03/2017 — v1.0: Initial publication*

Summary

On March 6, 2017, it has been reported that a remote code execution is possible via Apache Struts 2 framework, when performing file upload based on Jakarta multipart parser. There have been several exploits in the wild already reported [1], with some of them actually published publicly on Internet.

The fact that several experts have assessed this vulnerability as easy to exploit explains its popularity [2, 3]. This is also the reason, why it is recommended to upgrade to a patched version as soon as possible.

Technical Details

This vulnerability allows an attacker to send commands to the server running an unpatched version of Apache Struts 2 framework that will be executed with the privileges of the user running the service. According to the Apache documentation [1], this is possible by using a malicious `Content-Type` value.

This vulnerability has been assigned the number: CVE-2017-5638

Vulnerable Systems

- Apache Struts 2.3.5 - 2.3.31,
- Apache Struts 2.5 - 2.5.10.

Recommendation

Upgrade as soon as possible to Apache Struts 2.3.32 or Apache Struts 2.5.10.1

As a workaround, it is also possible to implement a servlet filter, which will validate `Content-Type` and throw away requests with suspicious values not matching multipart/form-data.

References

[1] Apache Org — https://cwiki.apache.org/confluence/display/WW/S2-045

[2] ArsTechnica — https://arstechnica.com/security/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites

[3] Cisco — http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html