Security Advisory Report - OBSO-1703-02

Apache Struts 2 RCE Flaw (CVE-2018-11776), Apache Struts2 Jakarta Multipart Parser File Upload Remote Code Execution (CVE 2017-5638)

Creation Date:	2017-03-28 16:11:00
Last Update:	2018-10-12 16:11:20

Summary

Update: new vulnerability

There is a new Apache Struts RCE Flaw that lets Hackers Take Over Web Servers

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

https://nvd.nist.gov/vuln/detail/CVE-2018-11776

Apache Struts versions 2.3 to 2.3.34 and 2.5 to 2.5.16 suffer from possible Remote Code Execution

known vulnerability

Apache Struts2 contains a flaw that is triggered when handling invalid Content-Type, Content-Disposition, or Content-Length values for uploaded files using the Jakarta Multipart parser.

This may allow a remote attacker to potentially execute arbitrary code.

Unify products do not use Apache Struts 2 and thus are not affected.

Details

Apache Struts is a free, open-source, MVC framework for creating elegant, modern Java web applications.
It favors convention over configuration, is extensible using a plugin architecture, and ships with plugins to support REST, AJAX and JSON.
http://struts.apache.org/index.html

A new critical vulnerability was found for Apache Struts2: (CVE-2018-11776)

Apache Struts versions 2.3 to 2.3.34 and 2.5 to 2.5.16 suffer from possible Remote Code Execution when alwaysSelectFullNamespace is true.

https://nvd.nist.gov/vuln/detail/CVE-2018-11776

Semmle security researcher Man Yue Mo has disclosed a critical remote code execution vulnerability in the popular Apache Struts web application framework that could allow remote attackers to run malicious code on the affected servers.

Apache Struts is an open source framework for developing web applications in the Java programming language and is widely used by enterprises globally, including by 65 percent of the Fortune 100 companies, like Vodafone, Lockheed Martin, Virgin Atlantic, and the IRS.

The vulnerability (CVE-2018-11776) resides in the core of Apache Struts and originates because of insufficient validation of user-provided untrusted inputs in the core of the Struts framework under certain configurations.

The newly found Apache Struts 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.

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

known vulnerability
A critical vulnerability was found for Apache Struts2: (CVE 2017-5638)
Attacks are based on commands injections into Struts servers that have not been patched yet.
The flaw resides in the Jakarta file upload multipart parser, which is a standard part of the framework and only needs a supporting library to function.
One series of commands that attackers are injecting into web pages stops the firewall protecting the server,
then downloads and executes malware of the attacker's choice.
The payloads include "IRC bouncers," which allow the attackers to hide their real IP address during Internet chats;
denial-of-service bots; and various other packages that conscript a server into a botnet.
These are several of the many examples of attacks that are currently being observed.
Affected are Web Servers using Jakarta based file upload Multipart parser for
Apache Struts 2.3.5 - Struts 2.3.31 and Struts 2.5 - Struts 2.5.10

Unify products do not use Apache Struts 2
Apache Struts1 is not affected
https://struts.apache.org/docs/s2-045.html

Affected Products

Unify products do not use Apache Struts 2 and thus are not affected.

Recommended Actions

No action is necessary concerning Unify products.

If a customer uses Apache Struts2 on his own he is advised to update it.

References

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

https://nvd.nist.gov/vuln/detail/CVE-2018-11776

http://thehackernews.com/2017/03/apache-struts-framework.html

http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html

https://cwiki.apache.org/confluence/display/WW/S2-045

https://struts.apache.org/docs/s2-045.html

http://blog.blackducksoftware.com/cve-2017-5638-apache-struts-2-vulnerability-security-news

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638

https://nvd.nist.gov/vuln/detail/CVE-2017-5638

https://community.rapid7.com/community/infosec/blog/2017/03/09/apache-jakarta-vulnerability-attacks-in-the-wild

https://www.exploit-db.com/exploits/41570/

Advisory: OBSO-1703-02, status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.
Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.