Indusface Security Bulletin

Apache Struts Remote Code Execution Vulnerability (CVE-2018-11776)

August 2018

What is Struts RCE Vulnerability (CVE-2018-11776)?

On August 22nd , Apache Foundation released a security update (S2-057) that fixes a critical remote code execution vulnerability in Apache Struts (CVE-2018-11776) affecting versions 2.3 to 2.3.34 and 2.5 to 2.5.16. The vulnerability was disclosed by security researcher Man Yue Mo from Semmle Security Research Team.

The vulnerability exists in the core of Apache Struts due to improper validation of user-provided untrusted inputs under certain configurations. Remote code execution is caused when using results with no namespace and in same time, its upper action(s) have no or wildcard namespace. Similar issue is caused when using url tag which doesn't have value and action set.

It is considered to be vulnerable if the following conditions are met.

- The alwaysSelectFullNamespace flag is set to true for Struts settings.
- In the Struts configuration file, you do not specify the optional namespace attribute, or it contains an "action" tag or "url" tag that specifies a wildcard namespace.

Successful exploitation could allow an attacker to execute remote code and possibly gain access to a targeted system.

What are the risks?

Struts is an open source, matured, web application framework based on the MVC design pattern and its widely being used in number of websites around the world including governments & enterprise companies. Semmle estimated that at least 65% of Fortune 500 companies use Struts in their web applications.

Considering Struts being used for publicly-accessible customer-facing websites, vulnerable systems are easily identified, and the flaw is easy to exploit (just by clicking an url) by an unauthenticated user.

As the flaw exists in the Struts framework core, all Struts installations are potentially vulnerable and hence it is likely to have wide implications for security across the Internet. Also, the vulnerability is related to the Struts OGNL language, which hackers are very familiar with, and are known to have been exploited in the past.

Working POC has been disclosed to public already and active attacks are most likely expected.

Severity: Critical

CVSSv2: Base Score 10
Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSSv3: Base Score 9.8
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Do I need to worry about it?

Vendor has released security patch and strongly advised to update their Apache Struts components to the latest version as soon as possible.

Mitigation:

Upgrade to Apache Struts version 2.3.35 or 2.5.17.

Configuration changes could be a temporary weak workaround. Verify that you have set (and always not forgot to set) namespace (if is applicable) for your all defined results in underlying xml configurations. Also verify that you have set (and always not forgot to 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.

Indusface Total Application Security (TAS) & AppTrana customers are automatically protected against RCE exploits by default. Customers are protected against CVE-2018-11776 and need not take any specific action for sites behind WAF. As best practice they are encouraged to upgrade their Apache Struts version at their convenience.