waratek

Customer Alert 20200903

Unpatched security holes in Apache Struts 2 can be exploited using freely available PoC code

Waratek can help secure vulnerable code without source code changes, upgrading, or downtime

Background

The US Cybersecurity and Infrastructure Security Agency (CISA) has issued an alert regarding CVE-2019-0230 and CVE-2019-0233, two Apache Struts 2 bugs that allow for remote code-execution and denial-of-service attacks on vulnerable installations. Apache Struts versions 2.0.0 through 2.5.20 of the popular open source platform are subject to a PoC exploit posted in August to GitHub.

Discussion

CVE-2019-0230 - According to the Apache Struts 2 Wiki, Struts frameworks, when forced, perform double evaluation of attributes' values assigned to certain tags attributes such as id so it is possible to pass in a value that will be evaluated again when a tag's attributes will be rendered. With a carefully crafted request, this can lead to Remote Code Execution (RCE).

The problem only applies when forcing OGNL evaluation inside a Struts tag attribute, when the expression to evaluate references raw, unvalidated input that an attacker is able to directly modify by crafting a corresponding request.

Example:

```
<s:url var="url" namespace="/employee" action="list"/><s:a id="%{skillName}" href="%{url}">List available Employees</s:a>
```

If an attacker is able to modify the skillName attribute in a request such that a raw OGNL expression gets passed to the skillName property without further validation, the provided OGNL expression contained in the skillName attribute gets evaluated when the tag is rendered as a result of the request.

The opportunity for using double evaluation is by design in Struts since 2.0.0 and a useful tool when done right, which most notably means **only referencing validated values in the given expression**. However, when referencing unvalidated user input in the expression, malicious code can get injected. In an ongoing effort, the Struts framework includes mitigations for limiting the impact of injected expressions, but Struts before 2.5.22 left an attack vector open which is addressed by this report.

CVE-2019-0233 - The Strust 2 Wiki notes that CVE-2019-0233 can be used in a Denial of Service (DoS) attack when performing a file upload. When a file upload is performed to an Action that exposes the file with a getter, an attacker may manipulate the request such that the working copy of the uploaded file is set to read-only. As a result, subsequent actions on the file will fail with an error. It might also be possible to set the Servlet container's temp directory to read only, such that subsequent upload actions will fail.

In Struts prior to 2.5.22, stack-accessible values (e.g. Action properties) of type java.io.File and java.nio.File as well as other classes from these standard library packages are not properly protected by the framework to deny access to potentially harmful underlying properties.

Action Steps

While the Apache Foundation recommends users upgrade to Struts v 2.5.22, it may not be feasible to upgrade applications with heavily modified open source code without breaking an apps functionality.

Waratek *Patch, Secure, and Upgrade* customers may request a virtual ARMR patch to fix the vulnerabilities identified in CVE-2019-0230 and CVE-2019-0233 by contacting their Client Services representative**.** Waratek's file, process forking, and input validation rules available in *Waratek Secure* and *Upgrade* also mitigate the attacks. **ARMR patches and rules install in minutes and do not require source code changes or app downtime.**

Non-Waratek customers should consider upgrading to Struts 2.5.22 and request a trial license or a live demonstration of the Waratek Patch.

About Waratek

Some of the world's leading companies use Waratek's ARMR Security Platform to patch, secure and upgrade their mission critical applications. A pioneer in the next generation of application security solutions, Waratek makes it easy for security teams to instantly detect and remediate known vulnerabilities with no downtime, protect their applications from known and Zero Day attacks, and virtually upgrade out-of-support Java applications – all without time consuming and expensive source code changes or unacceptable performance overhead.

Waratek is the winner of the 2020 Cyber Defense Magazine's Cutting Edge Award for Application Security, the Cybersecurity Breakthrough Award's 2019 Overall Web Security Solution of the Year, and is a previous winner of the RSA Innovation Sandbox Award along with more than a dozen other awards and recognitions.