CERT-EU Security Advisory 2017-017

Remote Code Execution Attack Against Apache Struts REST Plugin

September 7, 2017 — v1.0

History:

- *07/09/2017 — v1.0 – Initial publication*

Summary

On August 16th 2017, a new vulnerability affecting Apache Struts 2 (CVE-2017-9805) was published. Struts is a framework following the MVC model under Java working in Apache servers. This open-source framework is widely used to built web applications [1].

This vulnerability allows remote code execution attacks, when the Struts REST plugin is used with `XStreamHandler` to handle XML payloads. The problems is due to the lack of filters in the `XStreamHandler` when deserializing XML payloads.

It is important to note that the code that exploits the vulnerability has been released through Metasploit [2].

Products Affected

```
* Struts 2.1.2 - Struts 2.3.33,
* Struts 2.5 - Struts 2.5.12.
```

Recommendations

Fix is available through an upgrade to Apache Struts version 2.3.34 or 2.5.13.

It is important to take in consideration that this upgrade might require changes in the code of the applications supported by the plugin. It is recommended to follow the backward compatibility notes in the original Apache advisory [1].

As workarounds to consider:

1. Removing the Struts REST plugin, when not used.
2. Limiting the plugin to server normal pages and JSONs only. In order to do that proceed as follows:

- Disable handling of XML pages and requests to such pages

```
<constant name="struts.action.extension" value="xhtml,,json" />
```

- Override `getContentType` in `XStreamHandler`

```
public class MyXStreamHandler extends XStreamHandler { public String getContentType() {
 return "not-existing-content-type-@;/&%$#@";
 }
}
```

- Register the handler by overriding the one provided by the framework in your `struts.xml`

```
<bean type="org.apache.struts2.rest.handler.ContentTypeHandler" name="myXStreamHandmer"
  class="com.company.MyXStreamHandler"/>
<constant name="struts.rest.handlerOverride.xml" value="myXStreamHandler"/>
```

References

[1] https://cwiki.apache.org/confluence/display/WW/S2-052

[2] https://github.com/rapid7/metasploit-framework/pull/8924