Customer Alert 20170309

Waratek makes virtual patch available for new Struts 2 vulnerability CVE-2017-5638

Newly discovered flaw has existed for more than four years

The Apache Foundation announced a new vulnerability - CVE-2017-5638 - on Monday, March 6, 2017 and the first attacks exploiting the new vulnerability have already been reported. First introduced in Struts 2.3.5 released in October 2012, the vulnerability has been available for Zero Day exploits for more than four years.

Waratek is offering a Virtual Patch for customers to address the new high severity vulnerability that exposes organizations using the Struts 2 framework to any general code injection attack. The Waratek solution fully remediates this vulnerability with a virtual patch that can be live-updated without taking affected applications out of production.

“Struts 2 users need to take immediate action. Applying the binary patch offered by Apache requires some application downtime,” noted John Matthew Holt, Waratek’s Founder and CTO. “For users who have made custom changes on Struts source code, it could take days or weeks to upgrade. A virtual patch can be applied immediately while the application continues to run - with no code changes and without restarting the application.”

Even prior to the announcement of the vulnerability, Waratek’s core functionality protected against Proof-Of-Concept (POC) exploits of CVE-2017-5638 that perform remote-command execution. The new virtual patch is a specific one-line security rule that fully remediates this vulnerability and was developed in less than one-day after the vulnerability was announced.

“This is a critical vulnerability because the attack can be achieved without authentication, and web applications don’t necessarily need to successfully upload a malicious file to exploit this vulnerability,” advises Holt. “Just the presence of the vulnerable Struts library within an application is enough to exploit the vulnerability.”

Struts is an open source framework from the Apache Foundation used for web application development. Struts users include large-scale Internet companies, government, financial institutions and other enterprises around the world.

For more information, contact your account representative.
Two weeks after the Apache Foundation announced a previously unknown vulnerability in the Struts 2 web application framework, two new variations of the same vulnerability have been reported. However, Waratek customers who have applied the Virtual Patch for CVE-2017-5638 are already protected against the newly discovered variations as well as any possible other variation that might be discovered.

Background

According to the latest Struts 2 Security Bulletin (S2-046), it is possible to perform a Remote Command Execution (RCE) attack with a malicious Content-Disposition value or with improper Content-Length header. If the Content-Disposition / Content-Length value is not valid an exception is thrown which is then used to display an error message to a user. This is a different attack vector for the same vulnerability described in S2-045 (CVE-2017-5638).

Action Required

Waratek customers are protected against Code Injection and RCE attacks by the Waratek Application Security Platform’s standard protections such as Process Forking, Reflection Abuse, Name Space Layout Randomization (NSLR) feature. Waratek has also published a Virtual Patch for CVE-2017-5638 that is the functional equivalent to the physical patch offered by Apache and can be deployed safely on any version of Struts 2 without restart and no required source code or binary changes.

The Waratek Virtual Patch combined with Waratek’s Remote Command Execution mitigation, Reflection Abuse mitigation and NSLR features provides both an active and a reactive protection to the problem and removes the urgency to upgrade users who have customized the Struts 2 code used in web applications.

Companies who have not applied the Waratek Virtual Patch should review any temporary workarounds or security solutions that depend on pattern matching, heuristics, servlet filters, WAF-type protection. Security solutions that base detection on filtering the Content Type header or looking for unusual Content Type values will fail to mitigate the new exploits.

For more information, contact your account representative.