Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Kritische Schwachstelle in Apache Struts 2

CSW-Nr. 2018-218205-10k2, Version 1.0, 23.08.2018

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:WHITE: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Apache Struts [1] ist ein quelloffenes Model/View/Controller-Framework zum Entwickeln und Bereitstellen komplexer Java-basierter Webanwendungen. Es bietet Vorlagen für gängige Funktionen in Webanwendungen und setzt diese in Form von JavaServlets, JavaBeans, Resource Bundles und XML sowie verschiedenen Apache-Commons-Paketen um.

Im Apache Struts 2 Framework Core wurde eine Schwachstelle gefunden (CVE-2018-11776) [2,3], die einem Angreifer entfernte Codeausführung (RCE) ermöglicht.

Eine Verwundbarkeit besteht, wenn

1. in der Konfiguration von Struts für *alwaysSelectFullNamespace* der Wert "true" gesetzt ist. Gemäß [3] ist dies automatisch der Fall, wenn die Applikation das *Convention* Plugin verwendet und
2. innerhalb der Applikation Actions ohne Namespace oder mit einem Wildcard-Namespace konfiguriert sind (z.B. “//*/”). Dies gilt bspw. für in der Struts-Konfiguration oder in der Java-Codebasis definierte actions und namespaces (z.B. /<action namespace="main">/).

Ein anonymer Angreifer kann beim Aufruf einer zuvor von ihm manipulierten Webseite beliebige Befehle mit den Rechten des Webservers an das Betriebssystem übergeben. Verwundbar sind sowohl Windows-, als auch Unix-/Linux-Installationen der folgenden Apache Struts 2 Framework Versionen:

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

- Struts 2.3 - Struts 2.3.34
- Struts 2.5 - Struts 2.5.16

Eine Behebung der RCE-Schwachstelle ist in diesen Versionen erfolgt:

- Struts 2.3.35
- Struts 2.5.17

Bewertung

Dem BSI liegen derzeit keine Kenntnisse über eine aktive Ausnutzung der Schwachstelle vor.

Aufgrund der einfachen Ausnutzung und des durch eine vergleichbare Schwachstelle entstandenen Schadens (siehe auch CSW 2017-164920 vom 17.3.2017) ist die aktuelle Schwachstelle kritisch zu werten. Insbesondere sind die veröffentlichten Informationen für Angreifer ausreichend, um innerhalb kurzer Zeit Exploits zur Ausnutzung der Schwachstelle zu erstellen.

Maßnahmen

Aufgrund der kritischen Bewertung sollte bei Nutzung das Apache Struts 2 Framework, sofern noch nicht geschehen, schnellstmöglich auf die genannten Versionen aktualisiert werden.

Weitere Details finden sich unter [3].

Links

[1] Apache Struts Projekt-Webseite http://struts.apache.org/

[2] Apache Struts Advisory https://cwiki.apache.org/confluence/display/WW/S2-057

[3] Critical RCE Vulnerability in Apache Struts https://semmle.com/news/apache-struts-CVE-2018-11776

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs) welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

   Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

2) Welche Einstufungen existieren?

   - **TLP:WHITE: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
     Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.