2018 年 9 月 27 日

サービス＆セキュリティ株式会社 e-Gate センター

注意喚起：Apache Struts 2 の脆弱性を突いた攻撃について

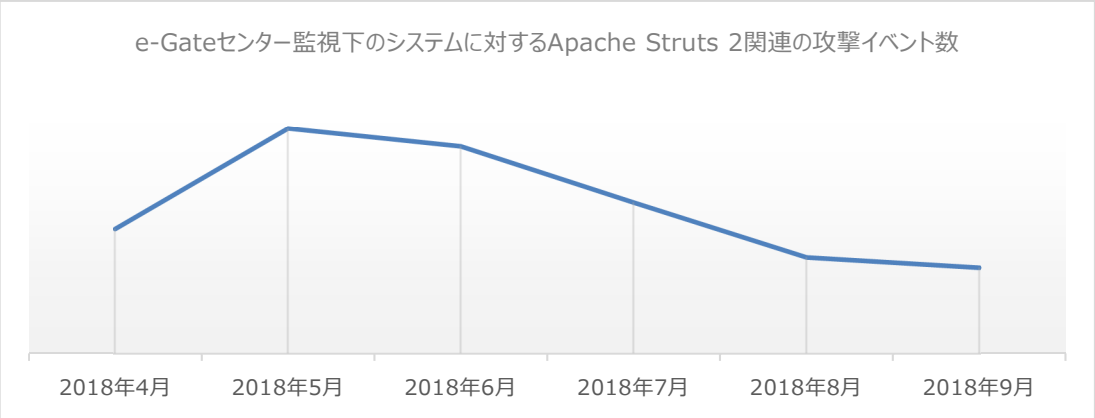
1. 概要

Apache Software Foundation が提供する Apache Struts 2 は、Java のウェブアプリケーションを作成するためのソフトウェアフレームワークです。フレームワークを使用することでアプリケーションの開発を効率よく進めることができます。ただし広く普及しているフレームワークは利便性に優れる一方で、攻撃の対象として狙われる可能性も高くなります。今回紹介する Apache Struts 2 は過去にも致命的な脆弱性が多数報告されております。

2018 年 8 月 24 日に IPA 及び JPCERT/CC によって Apache Struts 2 の脆弱性（CVE-2018-11776）について注意喚起が行われております。今回の脆弱性が悪用された場合、遠隔の第三者によって、サーバ上で任意のコードを実行される可能性があります。

IPA より、本脆弱性を悪用する攻撃コードが公開されているとの情報が発表されていますので、対策済みのバージョンへのアップデートや回避策を実施する必要があります。（後述の脆弱性情報を参照ください。）

e-Gate センターにおいても Apache Struts 2 に対するサイバー攻撃が確認されています。図 1 は e-Gate センターの監視するシステムにおける Apache Struts 2 に関連する攻撃イベント数の推移です。2018 年 5 月以降、イベント数は減少傾向にありますが、一定数の攻撃通信は継続しております。



【図 1　Apache Struts 2 関連の攻撃イベント数の推移】

2. 脆弱性情報詳細

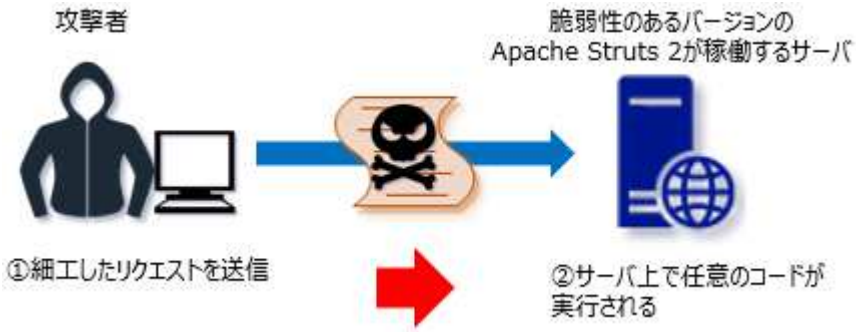
⑴ Apache Struts 2 (CVE-2018-11776)の脆弱性

対象となるバージョンで以下の条件の両方を満たす場合、本脆弱性の影響を受けます。

・alwaysSelectFullNamespace を true に設定している

・Struts 設定ファイル（struts.xml など）に、オプションの namespace 属性を指定しないか、ワイルドカードネームスペースを指定する "action"タグまたは "url"タグが含まれている場合

本脆弱性を悪用された場合、遠隔の第三者によって、サーバ上で任意のコードを実行される可能性があります。



【図 2 攻撃イメージ】

⑵ 対象となるバージョン

- Apache Struts 2
- 2.3 から 2.3.34
- 2.5 から 2.5.16

⑶ 対策

① 本脆弱性を修正した下記のバージョン以降のものに更新する。

Apache Struts 2.3.35

Apache Struts 2.5.17

② Struts の設定ファイル(strtuts.xml など)で namespace の値を指定し、URL タグの value と action の値を指定する。

③ 上記の更新や設定ファイルの修正ができない場合、IPS や WAF などをインターネットからの経路上に設置し、悪意のある攻撃を検知、遮断することができます。

⑷ 参考情報

■Apache Struts 2

Version Notes 2.5.17

https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.17

Version Notes 2.3.35

https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.3.35

Security Bulletins S2-057

https://cwiki.apache.org/confluence/display/WW/S2-057

■JPCERT/CC
Apache Struts 2 の脆弱性（S2-057）に関する注意喚起
http://www.jpcert.or.jp/at/2018/at180036.html
■独立行政法人情報処理推進機構（IPA）
Apache Struts2 の脆弱性対策について(CVE-2018-11776)(S2-057)
https://www.ipa.go.jp/security/ciadr/vul/20180823-struts.html

3. e-Gate の活用について

今回の攻撃は製品の脆弱性を狙った攻撃の一種です。サイバー攻撃を早期に発見する為には、対策(3)の③のようにセキュリティ機器を導入し、それらの機器の運用監視を行うことが重要です。SSK の総合セキュリティサービス「e-Gate」では、最新の分析システムを活用し精度の高い検知、また専任のアナリストによる分析を行っております。「e-Gate」のセキュリティ監視サービスをご活用頂くことにより迅速なセキュリティインシデント対応が可能となります。

■総合セキュリティサービス e-Gate
SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと、最新のメソッド、次世代 SOC“e-Gate センター“この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”です。e-Gate センターを核として人材・運用監視・対策支援という３つのサービスを軸に全方位のセキュリティサービスを展開しています。
【参考 URL】
https://www.ssk-kan.co.jp/e-gate/

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。リンク先のコンテンツは予告なく、変更、削除される場合があります。
※掲載した会社名、システム名、製品名は一般に各社の登録商標 または商標です。

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp