【Technical Report17-04】

2017 年 4 月 13 日

株式会社セキュアソフト

【続報】注意喚起：Apache Struts 2 の脆弱性情報と Sniper シリーズのシグネチャーリリースについて

1．概要

2017 年 3 月に Apache Struts 2 の脆弱性(S2-045)に関する注意喚起を掲載しましたが、1 か月経過した現在も本脆弱性を悪用した攻撃が増加傾向にあります。また、本脆弱性により国内でも個人情報漏洩などの被害報告が行われております。

2017 年 3 月 21 日に IPA より関連脆弱性として「S2-046」の注意喚起も行われており、より一層緊急度を上げた対応を実施する必要があります。（後述の参考情報を参照ください。）

2．脆弱性情報詳細

（1）対象となるバージョン

- Apache Struts 2.3.5 から 2.3.31 まで
- Apache Struts 2.5 から 2.5.10 まで

（2）対策

Apache Struts を以下の最新バージョンに更新する。

- Apache Struts 2.3.32
- Apache Struts 2.5.10.1

（3）対策までの対応方法

JPCERT/CC からは以下の対応方法が提示されています。

「Apache Software Foundation は、パーサをデフォルトの JakartaMultipart parser (JakartaMultiPartRequest) から変更することも対策として呼びかけています。速やかなアップデートが難しい場合は、本対策の適用をご検討ください。」

※上記方法では本脆弱性に対応できない事が確認された為、次の対応方法が提示されています。

1. 「Apache Software Foundation より、File Upload Interceptor を無効化する回避策が追加で案内されています。本回避策は、Struts 2.5.8 から 2.5.10 に対して有効とのことです。回避策を適用する場合は、十分な検証の上、実施してください。」

2. 「アドバイザリ（S2-046）で公開された脆弱性について、既に公開されているアドバイザリ（S2-045）と、脆弱性識別番号（CVE-2017-5638）は同じであり、修正バージョンの変更はありませんが、回避策（Jakarta Multipart parser/JakartaStreamMultiPartRequest の修正用プラグイン）が追加で案内されています。」

3. Sniper IPS, Sniper ONE での対策シグネチャーリリース

Sniper IPS, Sniper ONE シリーズは今回の脆弱性に対するシグネチャーをリリース致しました。
今回のようにシステムの脆弱性が見つかってもバージョンアップなどのシステム更新が必要で早急に対応できない場合に、Sniper IPS 等のセキュリティ製品による多層防御システムは有効です。

■ 3月9日 リリース（S2-045 対応）

シグネチャーコード	シグネチャー名
3431	Apache Struts2 Jakarta Multipart Parser RCE
3432	Apache Struts2 Jakarta Multipart Parser RCE.A

■ 3月29日 リリース（S2-046 対応）

シグネチャーコード	シグネチャー名
3440	Apache Struts2 Jakarta Multipart Parser RCE.B
3441	Apache Struts2 Jakarta Multipart Parser RCE.C
3442	Apache Struts2 Jakarta Multipart Parser RCE.D
3443	Apache Struts2 Jakarta Multipart Parser RCE.E
3444	Apache Struts2 Jakarta Multipart Parser RCE.F

＜参考情報＞

■Apache Struts 2

Version Notes 2.3.32
https://struts.apache.org/docs/version-notes-2332.html
Version Notes 2.5.10.1
https://struts.apache.org/docs/version-notes-25101.html
Struts Extras
https://struts.apache.org/download.cgi#struts-extras

■**Apache Struts 2 Documentation**

Possible Remote Code Execution when performing file upload based on Jakarta Multipart parser.
https://struts.apache.org/docs/s2-045.html
Possible RCE when performing file upload based on Jakarta Multipart parser (similar to S2-045)
https://struts.apache.org/docs/s2-046.html

■**JPCERT/CC**

Apache Struts 2 の脆弱性（S2-045）に関する注意喚起
https://www.jpcert.or.jp/at/2017/at170009.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-2017-5638)(S2-045)(S2-046)
https://www.ipa.go.jp/security/ciadr/vul/20170308-struts.html

«お問合せ先»
株式会社セキュアソフト
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-5464-9966
FAX 03-5464-9977
sales@securesoft.co.jp