2017 年 9 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

Apache Struts 2 の脆弱性情報に関する注意喚起のセキュリティニュースを 2017 年 3 月(TR17-03)と 4 月(TR17-04)に掲載しましたが、また新たに Apache Struts 2 の RCE※関連の脆弱性「CVE-2017-9805(S2-052)」が報告されました。

今回の脆弱性では、Apache Struts 2 で REST プラグインを有効に設定したサーバにて攻撃者がリモートで任意のコード（サーバーシャットダウン、バックドア設置等）を実行できる可能性があります。

2017 年 9 月 7 日に IPA にて、公開されている攻撃コードが動作する事が確認されている為、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。

※RCE(**R**emote **C**ode **E**xecution)・・・遠隔でのコード実行

2．脆弱性情報詳細

（1） Apache Struts2(CVE-2017-9805)の脆弱性

CVE-2017-9805 は、REST プラグインのデシリアライズ処理※において、細工された XML ペイロードを処理する際に任意のコードが実行可能になる脆弱性です。

※ デシリアライズ処理(Deserialization)： 送信されたデータを元のデータ形式に復元する処理

（2）対象となるバージョン

- Apache Struts 2.1.2 から 2.3.33 まで
- Apache Struts 2.5 から 2.5.12 まで

（3）対策

・Apache Struts を以下の最新バージョンに更新する。

- Apache Struts 2.3.34
- Apache Struts 2.5.13

・REST プラグインの削除や、XML 形式のリクエストを受け付けないよう制限する。

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 9 月 13 日付けでリリースいたしました。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。

今回、リリースしたシグネチャーは下記の通りです。

■9 月 13 日 リリース (S2-052 対応)

シグネチャーコード	シグネチャー名
3676	Apache Struts2 XStreamHandler RCE

＜参考情報＞

■Apache Struts 2

Version Notes 2.3.34

https://struts.apache.org/docs/version-notes-2334.html

Version Notes 2.5.13

https://struts.apache.org/docs/version-notes-2513.html

Struts Extras

https://struts.apache.org/download.cgi#struts-extras

■Apache Struts 2 Documentation

Possible Remote Code Execution attack when using the Struts REST plugin with XStream handler to handle XML payloads

https://struts.apache.org/docs/s2-052.html

■JPCERT/CC

Apache Struts 2 の脆弱性 (S2-052) に関する注意喚起

https://www.jpcert.or.jp/at/2017/at170033.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-2017-9805)(S2-052)

http://www.ipa.go.jp/security/ciadr/vul/20170906-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