Distributed via @police
http://www.npa.go.jp/cyberpolice/

平成 28 年4月 27 日

Topic

Apache Struts 2 の脆弱性を標的としたアクセスの観測について

Apache Struts 2 の脆弱性を標的としていると考えられるアクセスを観測しています。同ソフトウェアを利用している場合には、アップデートの実施等の適切な対策を早急に実施することを推奨します。

1 Apache Struts 2 の脆弱性について

平成 28 年4月 21 日に、Java 言語でウェブアプリケーションを開発する際に利用されるフレームワークである Apache Struts 2 に存在する深刻な脆弱性（S2-032、CVE-2016-3081）が、開発元である The Apache Software Foundation から公表[i]されました。開発元によると、当該脆弱性が悪用された場合、サーバ上で遠隔から任意のコードを実行させることが可能であるとされています。

また警察庁では、当該脆弱性の有無の調査や、脆弱性を悪用した攻撃が可能とみられる攻撃ツールが、インターネット上で複数公開されていることも確認しています。

2 Apache Struts 2 の脆弱性を標的としたアクセスの観測について

警察庁の定点観測システムにおいては、4月 27 日 02 時以降、当該脆弱性を標的としていると考えられるアクセスを観測しました（図1）。観測しているリクエストの中には、当該脆弱性が存在する機能へのアクセスを試みる内容が含まれているため（図2）、単に Apache Struts 2 が稼動しているサーバを探索する目的だけではなく、当該脆弱性の有無を探索したり、脆弱性を悪用した攻撃活動を実施したりする意図があるものと推測されます。

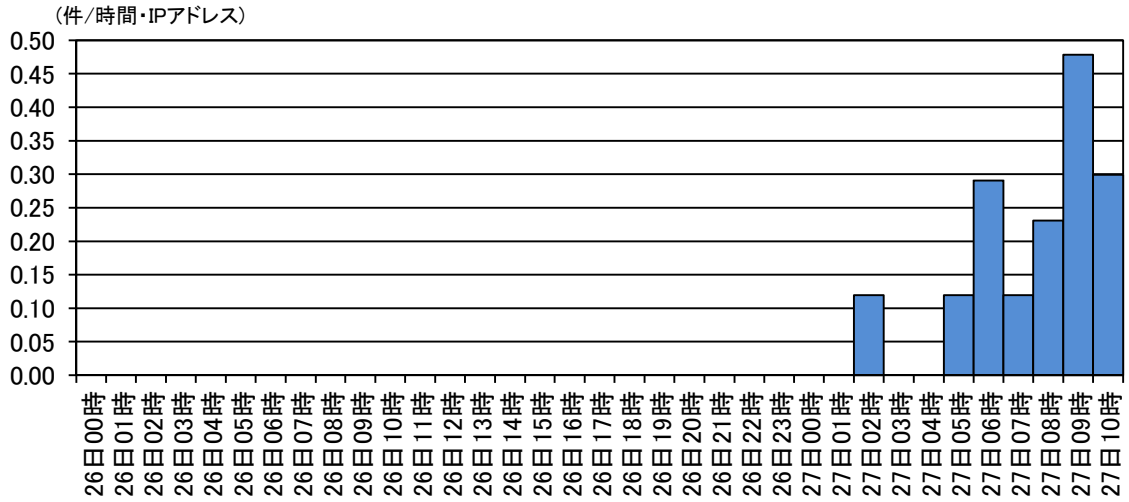

図1 Apache Struts 2 の脆弱性探索が目的と考えられるアクセス件数の推移
（4月 26 日 00 時～27 日 11 時）

[i] https://struts.apache.org/announce.html
https://struts.apache.org/docs/s2-032.html

図2　観測したリクエストの例（冒頭のみを抜粋、一部をマスキング）

3　推奨する対策

（平成 28 年4月 27 日 18 時追記）
　開発元のウェブサイトにおいて、バージョン情報の記載に変更が発生したため、一部修正を実施しました。

開発元によると、当該脆弱性の影響を受けるバージョンは以下のとおりです。

- Apache Struts 2.3.20 から 2.3.28（2.3.20.3、2.3.24.3 ~~2.3.20.2、2.3.24.2~~ は除く）

このため、脆弱性の影響を受けるバージョンの Apache Struts 2 を利用しているサーバの管理者は、当該脆弱性を修正した以下の最新バージョン（4月 19 日 12 時現在）への速やかなアップデート実施を推奨します。
　なお、速やかにアップデートすることが困難な場合には、開発元から一時的な回避策も公表されているため、必要に応じて検討を実施してください。

- Apache Struts 2.3.20.3 ~~2.3.20.2~~
- Apache Struts 2.3.24.3 ~~2.3.24.2~~
- Apache Struts 2.3.28.1

また、既に当該脆弱性が悪用された攻撃を受けている可能性も考えられるため、脆弱性が存在するバージョンの Apache Struts 2 を利用していた場合には、サーバの動作状況や、サーバ内の不審ファイルの有無等についても、併せて確認することを推奨します。