平成 26 年 4 月 27 日

Topic

Apache Struts2 の脆弱性を狙ったアクセスの検知について

Apache Struts2 の脆弱性を狙ったと考えられるアクセスを検知しています。同ソフトウェアを利用している組織においては、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 Struts2 の脆弱性を狙ったアクセスの検知について

平成 26 年3月2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 Struts2 に深刻な脆弱性[1]が明らかとなりました。脆弱性の公表と同時に、開発元から同脆弱性を修正するバージョンが公開されていましたが、修正が不十分であり同バージョンにも引き続き脆弱性が存在することが判明[2]しています。

同脆弱性が悪用された場合には、外部から細工したリクエストを送信することにより、機密情報の窃取や、ファイルの操作によるサイトの改ざん等が行われる危険性があります。4月 17 日には、攻撃の具体的な手順がインターネット上に公開されている旨も注意喚起[3]されています。

警察庁の定点観測システムにおいても、4月 26 日に、当該脆弱性を狙ったアクセスを観測しています。何者かが、脆弱性が存在するサーバを探索して、攻撃を試みている可能性が考えられます。

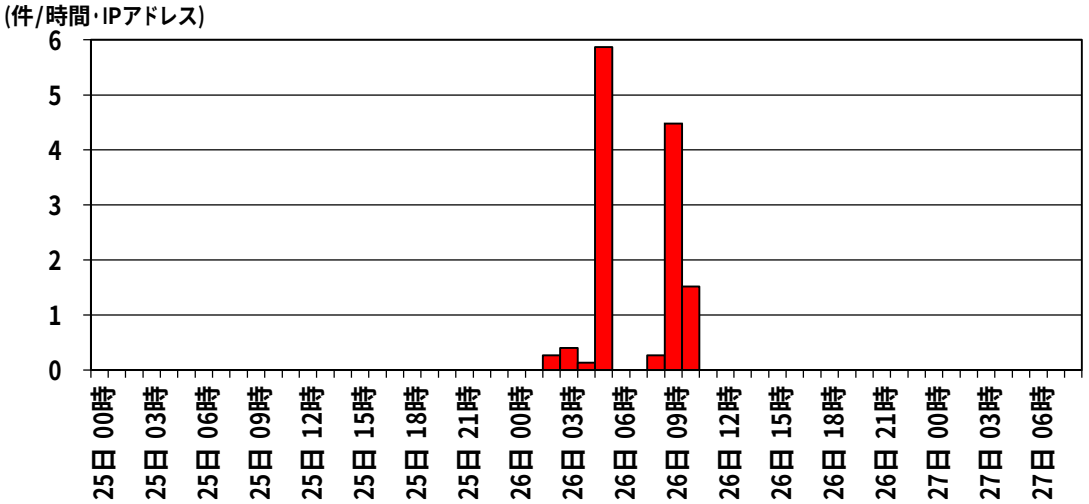

図1 Apache Struts2 の脆弱性を狙ったアクセスの検知状況
(H26.4.25 00:00～H26.4.27 08:59)

[1] 「JVNDB-2014-001603 Apache Struts の ParametersInterceptor における ClassLoader を操作される脆弱性」
http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-001603.html
[2] 「JVNDB-2014-000045 Apache Struts において ClassLoader が操作可能な脆弱性」
http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-000045.html
[3] 「更新：Apache Struts2 の脆弱性対策について(CVE-2014-0094)(CVE-2014-0112)」
http://www.ipa.go.jp/security/ciadr/vul/20140417-struts.html

2 推奨する対策

各組織においては、以下の対策を早急に実施することを推奨します。

⑴ 使用状況確認

各組織で管理するウェブサイトにおいて、Apache Struts の使用有無について確認を実施してください。

⑵ 対策の実施

Apache Struts を使用している場合には、次の対応を速やかに実施してください。

ア Apache Struts2 を使用している場合

4月 25 日に、脆弱性を修正した最新バージョンが公開されているため、アップデートを実施してください。

イ Apache Struts1 を使用している場合

Apache Struts1 については、既に開発元によるサポート期間が終了しており、脆弱性情報についても公表されていません。しかしながら、Apache Struts2 と類似する脆弱性が存在することが確認できたとの情報もあります。

Apache Struts1 を使用しているウェブサイトについては、公開を停止することを推奨します。その後、新たな環境への移行もしくは回避策の検証及び適用について、検討を実施してください。