— AUS（アルテミス・ユーザ・サポート）便り 2017/09/11号 —
https://www.artemis-jp.com

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●Struts2に新たな脆弱性…サーバ乗っ取りの可能性も

http://internet.watch.impress.co.jp/docs/news/1079383.html
http://www.ipa.go.jp/security/ciadr/vul/20170906-struts.html

このニュースをザックリ言うと･･･

- 9月5日（現地時間）、Apache Software Foundationより、Webアプリケーションフレームワーク「Apache Struts2」に複数の脆弱性が発見されたとして、修正バージョン（「2.5.13」および「2.3.34」）のリリースとともに警告が出されています。

- 特に危険とされる脆弱性（S2-052）は、外部から細工したXMLリクエストを送信することにより、サーバ上で任意のコードを実行することが可能とされ、攻撃者にWebサーバを乗っ取られる恐れがあるとされています。

- この他にもDoS攻撃が可能となる2件の脆弱性（S2-050・S2-051）が発見され、併せて修正されています。

- 既に脆弱性を悪用する攻撃コードが出回っている模様で、IPAのほかJPCERT/CCからも注意喚起が出され（http://www.jpcert.or.jp/at/2017/at170033.html）、速やかに最新バージョンへのアップデートが推奨されています。

AUS便りからの所感等

- Struts2は3月にも大きな脆弱性が発表されており、以降Struts2を採用しているWebサイトにおいて、その脆弱性を突かれたとみられる個人情報流出等の事件が連鎖的に発生していましたが、中には年度の予算による都合などから改修が遅れ、その間に攻撃を受けたケースもあります。

- Struts2を採用している企業等においては、是非ともこれまでの事件を教訓とし、速やかに改修を行い、それまでの間に発生する攻撃を遮断できるようWAFやUTMを設置、場合によっては改修までサイトを閉鎖するという判断も辞さない等の体制を整えることを強く推奨致します。

INTERNET Watch

「Apache Struts 2」に危険度の高いRCE脆弱性、修正バージョンの適用を推奨

岩崎 宰守　2017年9月6日 13:03

ツイート リスト いいね！32 シェア B! 11 Pocket 24

Apache Software Foundationは5日、「Apache Struts 2」について、危険度の最も高い"Critical"1件を含む脆弱性3件に関するアドバイザリを公開し、脆弱性を修正した最新バージョン「2.5.13」の提供を開始した。

Criticalと評価されているのは、リモートから任意のコードを実行できる（RCE：Remote Code Execution）脆弱性「S2-052」（CVE-2017-9805）。XStreamのハンドラにおけるXMLペイロード処理の問題によるもので、攻撃者がリモートから特別に細工を施したXMLリクエストを送信することで任意のコードを実行できるもの。RESTプラグインを使用しているバージョン「2.5」～「2.5.12」の環境で影響を受ける。

Apache Software Foundationでは回避策として、RESTプラグインの削除、またはXMLリクエストを受け付けないように制限することを挙げている。

このほかの脆弱性2件は、いずれもDoS攻撃が可能になるもの。「S2-050」（CVE-2017-9804）は、S2-047の修正が不完全だったもので、フォームに入力されたURLの検証不備によりDoS攻撃が可能になる。危険度は"Low"

一方の「S2-051」（CVE-2017-9793）は、RESTプラグインにおいてXstreamライブラリを使用しているときに、攻撃者がリモートから特別に細工を施したXMLリクエストを送信することで、DoS攻撃を実行できてしまうもの。危険度は"Medium"。

IPA Better Life with IT 情報処理推進機構

Apache Struts2 の脆弱性対策について(CVE-2017-9805)(S2-052)

最終更新日：2017年9月7日

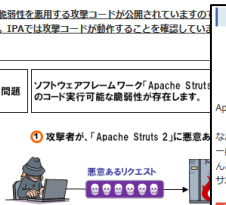
※追記すべき情報がある場合には、その都度このページを更新する予定です。

概要

Apache Software Foundation が提供する Apache Struts 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。
Apache Struts 2 には、REST プラグインを使用している場合に XML リクエストの処理に起因する、リモートで任意のコードが実行される脆弱性(CVE-2017-9805)が存在します。

本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。

本脆弱性を悪用する攻撃コードが公開されていますの
い。IPAでは攻撃コードが動作することを確認してい



図：脆弱性を悪用した攻撃のイメージ

影響を受けるバージョン

- Struts 2.1.2 から Struts 2.3.33, Struts 2.5 から Struts 2.5.12

なお、IPA では Apache Struts 2.3.33, 2.5.12 にて攻撃コードが動作することを確認しています。

Apache Struts 1 への影響は把握しておりません。

なお、「Apache Struts 1」は既に2013年4月5日を以ってサポートが終了しています。
一般的にサポートが終了した製品は脆弱性が判明した場合でも脆弱性対策の修正対応は実施されず、影響等の情報も公開されません。
サポート終了している「Apache Struts 1」をご利用の場合は利用を停止し、早急に移行をご検討ください。

Apache Struts 2 系のバージョンの確認方法例

Apache Struts 2 を利用しているウェブアプリケーションの /WEB-INF/lib ディレクトリを開き、その中の struts2-core-2.x.x.x.jar ファイルの名称を確認してください。
※ 2.x.x.x の部分が、利用している Struts 2 のバージョンです。

対策

脆弱性の解消 - アップデートする

開発者が脆弱性を修正した最新版を公開していますのでアップデートを実施してください。

Download a Release of Apache Struts - Struts 2.5.13
https://struts.apache.org/download.cgi#struts253
Download a Release of Apache Struts - Struts 2.3.34
https://struts.apache.org/download.cgi#struts-23x

●クレジットカード情報最大9458件流出、セキュリティコードも

https://netshop.impress.co.jp/node/4675

このニュースをザックリ言うと・・・

- 8月29日（日本時間）、ECサイト構築システムを提供する静岡県浜松市の業者より、同社のシステムを導入する18社のECサイトからクレジットカード情報が流出した可能性があると発表されました。

- 流出した情報は、3月23日～5月18日の間に決済を行ったクレジットカード最大9458件のカード番号、有効期限およびセキュリティコードとなっており、うち8件について不正利用が確認されているとのことです。

- 5月9日に決済代行会社から連絡を受けて同18日にカード決済を停止していましたが、その後のサーバの調査により、2009年3月以前に決済を行ったクレジットカード最大4851件のカード番号、有効期限、セキュリティコード、名義および電話番号が不適切に保管されていたことも確認され、流出した可能性があるとされています（不正利用は確認されていないとのことです）。

AUS便りからの所感等

- 3月23日にカード情報入力画面が改ざんされ、入力内容が海外のIPアドレスに送信される状態になっていたとのことで、時期的に見て3月に発覚したStruts2の脆弱性を突かれた可能性も考えられますが、定かではありません。

- 今回のような流出事件の多くにおいて、システムが被害を受けた業者は決済業務を「PCI DSS」に準拠する決済代行業者に委託し、カード情報を自前で保持しないよう改修していますが、カード情報に限らず、余分な情報を持たないようにすることは、万が一の流出時のリスクを抑えるためにも重要なことと言えます。

●メールを改ざんする新ハッキングテクニック、受信済みメールでも改ざん可能

http://gigazine.net/news/20170824-exploit-email-content/

このニュースをザックリ言うと・・・

- 8月22日（現地時間）、セキュリティベンダーのMimecast社の研究者より、電子メールによる新たな攻撃手法が確認されたとして同社ブログで警告が出されています。

- 記事において「Ropemaker」と名付けられたこの手法では、外部サイト上のCSSファイルを読み込むHTMLメールを送り付け、メールが受信された後でCSSファイルの内容を差し替えるというもので、これにより、メールを受信した時点では一見無害なURLが表示されていたものが、後で表示したときには悪意のあるURLを表示するようメールの内容をリモートから改変することが、アンチウイルス等にも検知されずに可能になるとしています。

- 記事の時点ではRopemakerを使った攻撃はまだ発見されていないとのことですが、「ただ検知されていないだけ」という可能性もあるとも指摘されており、回避策として、GMail・iCloud・Outlookなど、Webベースのメールクライアントを使うことを推奨しています。

AUS便りからの所感等

- HTMLメールは、当初メーラー（メールソフト）によっては悪意のあるスクリプトを実行される恐れ等があったことから敬遠されることも多々ありましたが、メーラー側でのセキュリティ対応や、Gmailをはじめとした安全で高機能のWebメールの登場で普及してきた経緯があります。

- 今回のRopemakerの手法が明らかになったことにより、攻撃者側が標的型攻撃メールにおいて採用する傾向が進むことが考えられる一方、対するメーラーやアンチウイルス・UTM等においても今後どのような対応がなされるかが注目されます。