報道関係各位

2014 年 5 月 1 日
株式会社アミティエ

Apache Struts の脆弱性（CVE-2014-0094）の回避策として、クラウド型 IPS＋WAF「攻撃遮断くん」を無償提供

株式会社アミティエ（東京都渋谷区、代表取締役 横田 武志、以下当社）は、当社が展開しているクラウド型 IPS＋WAF「攻撃遮断くん」を Apache Struts の脆弱性（CVE-2014-0094）の回避策としてご利用する場合に、無償でサービスを提供します。社会を揺るがす大問題に対して、「サイバー空間の安全安心を創造する」を理念として掲げているサイバーセキュリティ企業として、弊社ができる事は何かを熟考し、理念に基づき「攻撃遮断くん」を無償で提供することを決断しました。

※Apache Struts とは：Java を用いて Web アプリケーションを開発するためのフレームワークの一つ。オープンソースのソフトウェアで、誰でも自由かつ無償で利用・改変・再配布できる。官公庁や銀行、企業などで広く利用されている。

1.「CVE-2014-0094」に関して

Apache Struts（ストラッツ） に存在する脆弱性（欠陥）です。独立行政法人の情報処理推進機構（以下、IPA）や警察庁など、多くの機関より緊急の注意喚起がでています。
本脆弱性が悪用された場合は、個人情報や機密情報を盗まれたり、サイトを改ざんされたりする恐れがあります。Apache Struts 1 はサポートが終了しており、現在のところ本脆弱性の修正プログラム（パッチ）はありません。すでに攻撃方法がインターネット上で公開されており、早急に対策が必要です。

2.対策に関して

Apache Struts 1 においては、サポートが終了していますので、アップデートによる脆弱性の解消が不可です。IPA では回避策として、本脆弱性に対応したシグネチャを搭載した WAF（Web アプリケーションファイアウォール）や IPS（不正侵入防御システム）で攻撃リクエストを遮断する方法を推奨しています。
IPA：http://www.ipa.go.jp/security/ciadr/vul/20140417-struts.html

3.無償提供の背景

Apache Struts は多くの官公庁や企業で利用されています。警察庁は 2014 年 4 月 27 日、本脆弱性を狙ったアクセスを検知したとして注意を呼びかけており、Apache Struts 1 を使用している WEB サイトについては、公開を停止することを推奨しています。すでに悪影響は広がっており、例えば国税庁は 2014 年 4 月 25 日、Web サイト上の「確定申告書作成コーナー」など 3 つのサービスを停止しました。しかしながら、多くの官公庁や企業では WEB サイトの公開停止は難しく、悪影響が広がる事が懸念されます。

4.攻撃遮断くんの無償提供に関して

Apache Struts の脆弱性（CVE-2014-0094）の回避策としてご利用の場合、最大2ヶ月（申込み日の翌月末まで）無償でご利用頂けます。お申込後、最短3営業日（通常5営業日）でサービス提供いたします。
※攻撃遮断くんは本脆弱性（CVE-2014-0094）に対応したシグネチャを搭載しております。
※限定100社。
お申込URL：https://www.amitie-hd.com/contact/

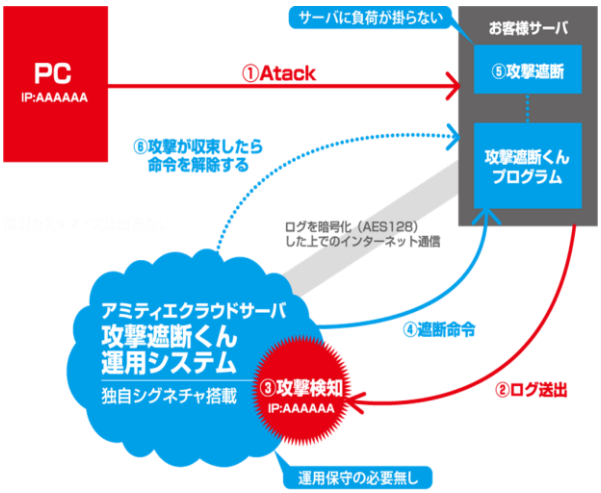
攻撃遮断くん

【参考：サービス概要】

クラウド型 IPS＋WAF「攻撃遮断くん」は、外部公開サーバへのあらゆる攻撃を遮断するクラウド型のサーバセキュリティサービスです。WEB 改ざん、情報漏洩、踏み台、サービス妨害等の被害を防ぐ事が出来ます。BIGLOBE クラウドホスティングの IPS オプションや BBTower クラウドセキュリティサービスに選定されるなど、大変好評いただいております。

革新的な攻撃遮断くんの仕組み
攻撃遮断くんプログラムは、各種ログを攻撃遮断くん運用システムに送出し、シグネチャに合致する不正アクセスだった場合に出される、遮断命令を実行するのみにする事で、 主な特徴を実現しています。

＜主な特徴＞
・ネットワーク構成の変更やサーバ停止の必要なし
・ご担当者様での保守・運用作業は一切必要なし
・シグネチャは自動で最新にアップデート
・クラウド環境（IaaS）への対応
・ほぼすべての OS に対応
・サーバへの負荷は1％以下
・攻撃可視化＋コンサルティング
・5 営業日でサービス開始可能



＜詳細＞
◆サービス内容
・24 時間 365 日のセキュリティ監視
・サイバー攻撃の検知・遮断及び
・担当者さまへのメール報告
・月ごとのセキュリティレポート提供
・セキュリティについてのアドバイス

◆対応可能な主なサイバー攻撃
ブルートフォースアタック（総当り攻撃）・DDos 攻撃・SQL インジェクション・クロスサイトスクリプティング
ディレクトリトラバーサル・OSコマンドインジェクション・改行コードインジェクション
その他、サーバ OS・WEB サーバソフト・WEB アプリケーション層を狙った多くの攻撃に対応しています。

◆サービス提供対象
Web サーバ、メールサーバ、FTP サーバ、ファイルサーバ、その他インターネットに繋がるサーバ全般

◆対応 OS
Linux の全てのディストリビューション・FreeBSD (all versions) ・OpenBSD (all versions)
NetBSD (all versions) ・Solaris 2.7, 2.8, 2.9, 10 and 11 ・AIX 5.3, 6.1 and 7.1 ・HP-UX 10, 11, 11i
Windows 8, 7, XP, 2000 and Vista ・Windows Server 2003, 2008 and 2012 ・MacOSX 10

◆仮想サーバへの対応
VMware・KVM・Hyper-V・Xen・OSS etc

◆利用料金
初期費用：10,000 円　 月額利用費用：40,000 円
・課金単位：1グローバル IP（サーバから見て OUT 側の通信で使用されるグローバル IP 毎）
・上記価格に消費税は含まれておりません。