プレスリリース
2014 年 10 月 9 日
独立行政法人情報処理推進機構

脆弱性攻撃検出ツール「iLogScanner」 に不正アクセスの兆候検出機能を追加

～同時公開の“オフライン版”では自組織ニーズに合わせたカスタマイズや解析の自動化も可能～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、「ウェブサイトの脆弱性攻撃検出ツール iLogScanner」に、不正アクセスの兆候を検知する機能およびネットワークにつながずに機能を使用するオフライン版を追加し、「ウェブサイトの攻撃兆候検出ツール iLogScanner」として 2014 年 10 月 9 日から IPA のウェブサイトで公開しました。
URL： https://www.ipa.go.jp/security/vuln/iLogScanner/

2013年は日本国内におけるウェブサイトの改ざんが急増し(*1)、2014年に入っても官公庁や出版社、大学などの様々なウェブサイトが改ざんされる事件が後を絶ちません。ウェブサイト改ざんの手口(*2)には、(1) 「ウェブアプリケーションの脆弱性の悪用」や (2) 「総当たり攻撃(*3)やパスワードリスト型攻撃(*4)を仕掛け、不正アクセスを行う」などがあります。特に、国内外の中小企業を狙った不正アクセスの47%は総当たり攻撃によるものといった調査結果(*5)も出ており、ウェブサイト管理者は、改ざんを防ぐための適切な対策が求められています。

「iLogScanner(*6)」はウェブサイトの運営・管理にコストをかけることが難しい組織の利用を想定し、上記(1) の兆候をウェブサーバーのログから検知する機能を提供することを目的としており、2008 年 4 月より公開しています。今回の機能強化は、(2) の不正アクセスの兆候の検知機能の提供を主としています。また、従来のオンライン版に加え、iLogScanner をインターネット経由でなく利用者のパソコンにインストールして使用するオフライン版の提供を開始しました。概要は下記の通りです。

（1）新たに不正アクセスの兆候を検知する機能を追加（別紙① 参照）

ウェブサーバーに蓄積されたログから、iLogScanner を使って攻撃の有無の判断に有効なログを抽出、解析する機能を新たに追加しました。抽出するログには例えば、ウェブアプリケーションへのアクセス時刻、ウェブサーバーへのアクセス元 IP アドレス、管理者アカウント（root）への権限昇格の有無などがあります。ウェブサイトの管理者は定期的に本ツールでログを解析し、出力されたレポートから、業

(*1) 2013 年 9 月 6 日 ウェブサイト改ざん等のインシデントに対する注意喚起:
http://www.ipa.go.jp/security/topics/alert20130906.html
(*2) IPA テクニカルウォッチ「ウェブサイト改ざんの脅威と対策」(IPA):
http://www.ipa.go.jp/security/technicalwatch/20140829.html
(*3) ログイン ID やパスワードなどに対して理論的にありうるパターン全てを機械的に入力してログインを試みる攻撃。ブルートフォースアタック（Brute-force attack）とも呼ばれる。
(*4) あらかじめ入手しリスト化したログイン ID とパスワードを利用してログインを試みる攻撃
(*5) 2013 年度データ漏洩/侵害調査報告書(ベライゾンジャパン合同会社) P34:
http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_ja_xg.pdf
(*6) 利用者はインターネット経由で IPA のサイトにある iLogScanner にアクセスして利用する。

務時間外のウェブアプリケーションへのアクセスや、管理者権限が昇格されたなどの現象を確認し、不正アクセスの兆候の有無を確認することが出来ます。これにより、もし不正アクセスが疑われる場合は、運用管理用アプリケーションの一時停止やパスワード(認証情報)の変更などの対策の検討が可能となります。

なお、この新機能は、SSH（エスエスエイチ）[*7]やFTP（エフティーピー）[*8]などの仕組みが利用された運用管理アプリケーションに対する攻撃を対象としています。

（2）利用者がカスタマイズして利用できる iLogScanner オフライン版の提供　（別紙②　参照）

オフライン版はインターネット経由でログを解析することに抵抗を覚えたり、解析作業を自動化したいというニーズに応え、提供を開始しました。iLogScanner をネットワークに接続することなく自組織でカスタマイズして使用できますので、ウェブサイト管理者は攻撃の兆候を検知する作業を自動化させ、運用管理を省力化することができます。

IPA では、本ツールが企業や様々な組織で活用され、ウェブサイトが安全に運営されることを期待すると共に、ウェブサイトのセキュリティ対策の一助となるよう、今後とも普及・啓発を推進していきます。

■ 本件に関するお問い合わせ先
IPA 技術本部 セキュリティセンター　亀山／土屋
Tel: 03-5978-7527　Fax: 03-5978-7518　E-mail: vuln-inq@ipa.go.jp
■ 報道関係からのお問い合わせ先
IPA 戦略企画部　広報グループ 横山／白石
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp

[*7] SSH（Secure Shell）：暗号や認証の技術を利用して、安全にリモートコンピュータと通信するためのプロトコル。
[*8] FTP（File Transfer Protocol）：ネットワーク上でファイルを転送するためのプロトコル。