JPCERT CC®
Japan Computer Emergency Response Team Coordination Center
JPCERTコーディネーションセンター

旧バージョンの Parallels Plesk Panel の利用に関する注意喚起

最終更新: 2013-04-08

各位

JPCERT-AT-2013-0018
JPCERT/CC
2013-04-08

<<< JPCERT/CC Alert 2013-04-08 >>>

旧バージョンの Parallels Plesk Panel の利用に関する注意喚起

https://www.jpcert.or.jp/at/2013/at130018.html

I. 概要

JPCERT/CC では、サーバ上に不正な Apache モジュールが設置されたことにより、Web サイト閲覧時に意図しない JavaScript が挿入される Web 改ざんに関する報告を多数受けています。改ざんされたサイトを閲覧した場合、結果としてユーザの PC がマルウエアに感染する可能性があります。

弊センターにて入手した情報によると、これらのサイトでは、サポート期限切れのバージョンを含む旧バージョンの Parallels Plesk Panel が多く使われているとのことです。Parallels Plesk Panel が稼働しているサーバには、付随する様々なソフトウエア(MySQL、BIND、phpMyAdmin 等)がインストールされている可能性があり、ユーザはこれらのソフトウエアを使用している認識が薄いため、脆弱性を内在した古いバージョンで稼働している場合が多くあります。

今回の不正な Apache モジュール設置に関する Web 改ざん事例の全てが脆弱性を起因とするものであるとは確認できていませんが、脆弱性を内在した状態で運用を行っている場合、攻撃者によって脆弱性を突かれ、Web 改ざんなどの被害を受ける可能性がありますので、未然防止の観点から、Parallels Plesk Panel 本体だけでなく、OS や製品に含まれるその他のソフトウエアも含め、最新の状態にアップデートすることをお勧めします。

一部の攻撃では、旧バージョンの Parallels Plesk Panel に存在する SQL インジェクションの脆弱性を用いてアカウント情報が窃取されたり、初期設定のパスワードや簡易なパスワードを設定している場合には辞書攻撃によりアカウント情報が特定されて、不正なログインが行われている事例を確認しています。また、ログイン後、Parallels Plesk Panel の cron manager 機能を用いて不正なスクリプトを動作させ、結果として不正な Apache モジュールが設置されている事も確認しています。

II. 対策

Web サイトの管理用に Parallels Plesk Panel を使用している場合は、以下の対策をご検討ください。

- Parallels Plesk Panel を最新のバージョンに更新する
- サーバに含まれる OS、ソフトウエアを最新に更新する
- Parallels Plesk Panel へのアクセス制限を行う
  (特定の IP アドレスに限定するなど)

- 安全性の高いパスワードを設定する
- 使用する Parallels Plesk Panel の設定画面から root 権限でのタスク実行を禁止する(*1)

(*1) 初期設定では、Parallels Plesk Panel は以下のケースで、ユーティリティやスクリプトを root 権限で実行することを許可しています。
- cron manager でのタスクのスケジューリング (バージョン 8 ～ 11)
- Event Manager tool でのイベントハンドリング (バージョン 11)

これらの操作を禁止するためには、以下のパス及びファイル名で空ファイルを作成してください。$PRODUCT_ROOT_D は、RPM ベースのシステムでは /usr/local/psa、DEB ベースのシステムでは /opt/psa と読み替えてください。

$PRODUCT_ROOT_D/var/root.crontab.lock
$PRODUCT_ROOT_D/var/root.event.handler.lock

詳細は以下の「Protecting from Running Tasks on Behalf of root」を参照してください。

Enhancing Security
http://download1.parallels.com/Plesk/PP11/11.0/Doc/en-US/online/plesk-linux-advanced-administration-guide/68755.htm

III. 参考情報

Parallels
Parallels Plesk Panel 11.0 for Linux リリースノート
http://download1.parallels.com/Plesk/PP11/11.0/release-notes/ja-JP/parallels-plesk-panel-11.0-for-linux-based-os.html

Parallels
Parallels Plesk Panel のセキュリティに関するベストプラクティス
http://kb.parallels.com/jp/114620

Parallels
Enhancing Security
http://download1.parallels.com/Plesk/PP11/11.0/Doc/en-US/online/plesk-linux-advanced-administration-guide/68755.htm

トレンドマイクロ
国内外におけるWebサーバ（Apache）の不正モジュールを使った改ざん被害
http://blog.trendmicro.co.jp/archives/6888

今回の件につきまして当方まで提供いただける情報がございましたら、ご連絡ください。

==========
一般社団法人 JPCERT コーディネーションセンター (JPCERT/CC)
MAIL: info@jpcert.or.jp
TEL:03-3518-4600 FAX: 03-3518-4602
https://www.jpcert.or.jp/