

Ruby on Rails の Action Pack のパラメータ解析の脆弱性により 任意の Ruby コードを実行される脆弱性 (CVE-2013-0156) に関する検証レポート

2013/1/24

NTT データ先端技術株式会社

辻 伸弘

小松 徹也

【概要】

Ruby on Rails に、リモートより任意のコードを実行される脆弱性が発見されました。この脆弱性は、パラメータ解析における YAML およびシンボル変換の不備に起因します。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、奪取したユーザ権限で任意の Ruby コードの実行が可能です。

今回、この Ruby on Rails の Action Pack のパラメータ解析の脆弱性により、任意の Ruby コードを実行される脆弱性 (CVE-2013-0156) の再現性について検証を行いました。

検証環境には、HTTP リクエストを処理するための Web サーバと Web アプリケーションフレームワークとして Ruby on Rails を使用する Rails アプリケーションを使用しております。

【影響を受けるとされているシステム】

- Ruby on Rails 3.2.10 およびそれ以前のバージョン
- Ruby on Rails 3.1.9 およびそれ以前のバージョン
- Ruby on Rails 3.0.18 およびそれ以前のバージョン
- Ruby on Rails 2.3.14 およびそれ以前のバージョン

【対策案】

Ruby on Rails Project より、この脆弱性を修正するバージョンがリリースされています。当該脆弱性が修正されたバージョンにアップデートしていただくことを推奨いたします。

Ruby on Rails ダウンロードサイト

<http://rubyonrails.org/download>

- Ruby on Rails 3.2.11
- Ruby on Rails 3.1.10
- Ruby on Rails 3.0.19
- Ruby on Rails 2.3.15

【参考サイト】

CVE-2013-0156

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0156>

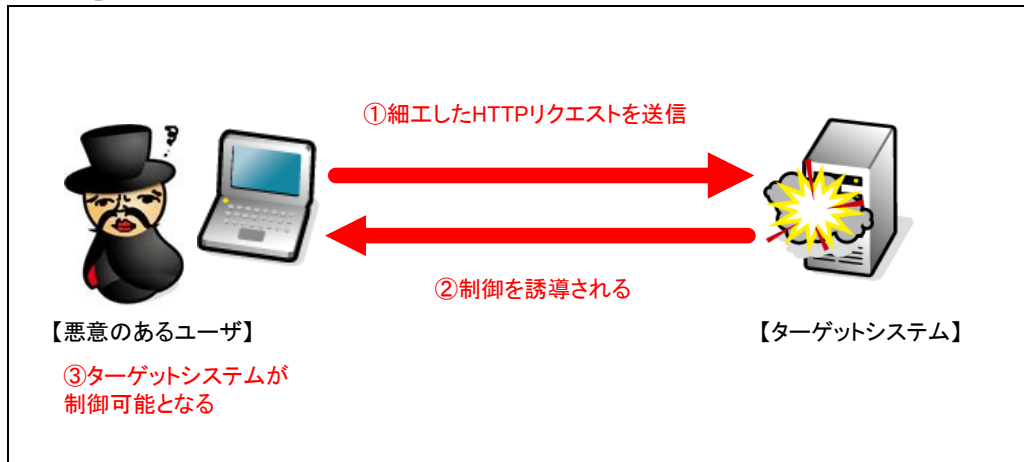
Vulnerability Note VU#380039

<http://www.kb.cert.org/vuls/id/380039>

JVNVU#94771138: Ruby on Rails に複数の脆弱性

<http://jvn.jp/cert/JVNVU94771138/>

【検証イメージ】



【検証ターゲットシステム】

・Debian 6.0.6 上の Ruby on Rails 3.2.10

※Web サーバおよび Ruby on Rails アプリケーションを検証環境に含みます。

【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、Ruby on Rails を利用したアプリケーションを介して、任意の Ruby 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 Windows 7 です。

【検証結果】

下図は、攻撃後の誘導先のシステム画面です。

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 (Windows 7) のターミナル上にターゲットシステム (Debian) 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奪取に成功した画面

```
cmd コマンドプロンプト - nc.exe -lp 4444
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>nc.exe -lp 4444

id
uid=0(root) gid=0(root) groups=0(root)

uname -a
Linux rails 2.6.32-5-686 #1 SMP Sun Sep 23 09:49:36 UTC 2012 i686 GNU/Linux

rails -v
Rails 3.2.10

ruby -v
ruby 1.9.2p0 (2010-08-18 revision 29036) [i486-linux]

ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0c:29:0d:98:eb
          inet addr:10.0.0.106  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe0d:98eb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:23711 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14289 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21696580 (20.6 MiB)  TX bytes:2610273 (2.4 MiB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
```

* 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>