

Ruby on Rails の JSON のパラメータ解析の脆弱性により 任意のコードを実行される脆弱性(CVE-2013-0333)に関する検証レポート

2013/2/1

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、JavaScript Object Notation (JSON) パラメータ解析における JSON から YAML への変換不備に起因します。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、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 Ruby on Rails の JSON のパラメータ解析の脆弱性により任意のコードを実行される脆弱性 (CVE-2013-0333) 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 3.0.19 およびそれ以前のバージョン
- Ruby on Rails 2.3.15 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 3.0.20
- Ruby on Rails 2.3.16

【参考サイト】

CVE-2013-0333

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0333>

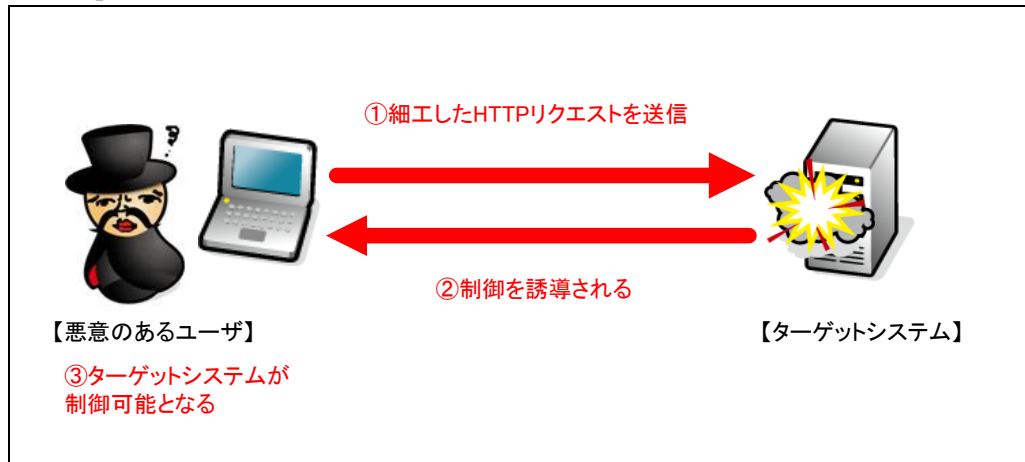
Vulnerability Note VU#628463: Ruby on Rails 3.0 and 2.3 JSON Parser vulnerability

<http://www.kb.cert.org/vuls/id/628463>

JVNDB-2013-001320: Ruby on Rails における任意のコードを実行される脆弱性

<http://jvndb.jvn.jp/ja/contents/2013/JVNDB-2013-001320.html>

【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 3.0.19

※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、Web サーバの動作権限で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 *Ubuntu 10* 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 (Ubuntu 10) 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

```
root@bt:~# uname -a
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux
root@bt:~#
root@bt:~# nc -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 3.0.19

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

ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:0d:98:eb
          inet addr:192.168.195.79  Bcast:192.168.195.255  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:118266 errors:0 dropped:0 overruns:0 frame:0
          TX packets:41196 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:147843237 (140.9 MiB)  TX bytes:4381164 (4.1 MiB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
```

* 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>