

Movable Type の mt-upgrade.cgi プログラムの欠陥により 任意のコードを実行される脆弱性(CVE-2013-0209)に関する検証レポート

2013/1/28

NTT データ先端技術株式会社

辻 伸弘

渡邊 尚道

【概要】

Movable Type 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、アップグレード関連プログラムである mt-upgrade.cgi にて使用されている、lib/MT/Upgrade.pm 関数の、エスケープ処理に不備があるために発生します。

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 OS のコマンドおよび SQL クエリを実行することが可能です。

今回、この Movable Type の mt-upgrade.cgi プログラムの欠陥により任意のコードを実行される脆弱性 (CVE-2013-0209) 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 サーバとデータベースを使用しています。

【影響を受けるとされているシステム】

- Movable Type 4.2x 系全てのバージョン
- Movable Type 4.31 から 4.38 のバージョン

【対策案】

シックス・アパート社より本脆弱性が修正された Movable Type 5.x 系がリリースされております。5.x 系へアップデートしていただくことを推奨します。4.38 については修正プログラムがリリースされておりますが 4.3x 系はサポートが本年限りの予定であるためベンダーは 5.x 系へのアップデートを推奨しています。
また、4.2x 系は既にメンテナンスを停止しております。

ダウンロードサイト

-シックス・アパート社

<http://www.sixapart.jp/movabletype/>

-Movable Type 4.38 patch to fix a known upgrading security issue

http://www.movabletype.org/2013/01/movable_type_438_patch.html

また、アップデートしない場合の回避策として、原因となっている mt-upgrade.cgi プログラムの削除、または実行権限の無効化により脆弱性を回避することができます。

このアクションについてシックス・アパート社は脆弱性の有無に関わらず推奨しています。

Q. インストールが終了したら削除するファイルはありますか

<http://www.movabletype.jp/faq/post-7.html>

【参考サイト】

CVE-2013-0209

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0209>

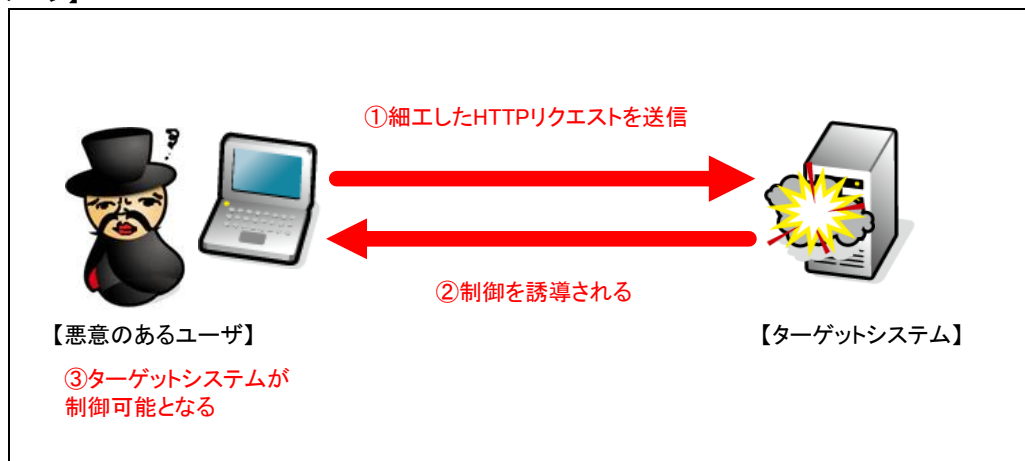
National Vulnerability Database (CVE-2013-0209)

<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0209>

JVNDB-2013-001237

<http://jvndb.jvn.jp/ja/contents/2013/JVNDB-2013-001237.html>

【検証イメージ】



【検証ターゲットシステム】

・Debian 6.0.6 上の Movable Type 4.38-ja

※Web サーバ・データベース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、Movable Type の mt-upgrade.cgi 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が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に示すように、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に示すように、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

```
C:\Windows\System32\cmd.exe - nc.exe 192.168.204.186 1234
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\System32>nc.exe 192.168.204.186 1234
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a
Linux debian 2.6.32-5-686 #1 SMP Sun Sep 23 09:49:36 UTC 2012 i686 GNU/Linux
/sbin/ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:df:40:4e
          inet addr:192.168.204.186  Bcast:192.168.204.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fedf:404e/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:72562 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27947 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:67789568 (64.6 MiB)  TX bytes:2452405 (2.3 MiB)
          Interrupt:19 Base address:0x2000
```

* 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>