

# GNU Bash 취약점 대응 방안

2014.09

펜타시큐리티시스템(주)

# 목차

## I. 개요

## II. 취약점 상세

1. CVE-2014-6271 취약점 이란?
2. CVE-2014-6271 취약점의 영향도
3. CVE-2014-6271 취약점 유무 확인 방법

## III. 대응 권고 방안

1. 패치 방안
2. Web Server 취약점 대응 방안
3. 상세 설정

# I. 개요

## 목적

- GNU Bash (Bourne Again Shell) 환경 변수를 통한 command Injection 취약점 대응

## 취약점 대상

- GNU Bash (Bourne Again SHell)
- 특정 취약 조건 : Bash로 짜여진 CGI 페이지

## 취약점 관련 공격 내용

- Bash Shell을 사용하는 CGI 코드의 원격 실행

## CVE 정보

- CVE-2014-6271 (GNU Bash 원격 코드 실행 취약점)
  - 2014년 09월 24일 발표

## II. 취약점 상세 (1/3)

### 1. CVE-2014-6271 취약점 이란?

- <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271>
- 공격자가 악의적인 명령어가 포함된 조작된 환경 변수를 사용하여 GNU Bash 원격코드 실행 취약점 공격에 성공할 경우, 해당 공격으로 인해 악의적인 코드 및 명령이 실행 가능해지며, 공격자는 표적 컴퓨터를 제어할 수 있게 됩니다.
  - Bash의 환경 변수에 함수 정의를 이용해서 원하는 코드를 추가할 수 있고, 다음 Bash가 사용될 때, 추가된 코드가 실행되는 취약점
  - Bash는 사용자가 명령어를 간단한 텍스트 기반의 윈도우에 입력하면 OS가 이에 따라 동작하게 하는 명령어 해석기의 역할을 수행
- 공격 예
  - Bash 형태로의 환경 변수를 저장하는 별도의 어플리케이션이 존재할 경우, 아래와 같이 Bash를 사용하는 다른 프로그램에서 환경 변수 설정 값을 변경하여 악의 있는 공격이 가능합니다.

```
neozizz ~ # env ABC='() { 6261;}; cat /etc/passwd' bash -c ''
#root:x:0:0:root:/root:/bin/bash
root:x:0:0:root:/root:
bin:x:1:1:bin:/bin:/bin/false
daemon:x:2:2:daemon:/sbin:/bin/false
adm:x:3:4:adm:/var/adm:/bin/false
lp:x:4:7:lp:/var/spool/lpd:/bin/false
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/bin/false
news:x:9:13:news:/usr/lib/news:/bin/false
uucp:x:10:14:uucp:/var/spool/uucppublic:/bin/false
operator:x:11:0:operator:/root:/bin/bash
man:x:13:15:man:/usr/share/man:/bin/false
postmaster:x:14:12:postmaster:/var/spool/mail:/bin/false
smmisp:x:209:209:smmsp:/var/spool/mqueue:/bin/false
portage:x:250:250:portage:/var/tmp/portage:/bin/false
nobody:x:65534:65534:nobody:/bin/false
```

## II. 취약점 상세 (2/3)

### 2. CVE-2014-6271 취약점의 영향도

#### ■ WAPPLES에 대한 영향도 => 없음

- CLI모드 의 경우, 관리자만 접근하는 형태로 IP접근제어를 하고 있고 별도 VTY shell 기반으로 동작 하기 때문에 별도 Bash 호출을 하지 않습니다.
- 관리페이지 WEB이나, 관리도구에서 Bash 형태로 환경 변수를 받을 수 있는 부분이 없습니다.

#### ■ Web Server에 대한 영향도 => (부분적으로) 있음

- CGI에서 Web Server의 환경변수를 호출할 수 있도록 Bash가 제공되고 있기 때문에, 만약 Bash로 개발되어 있는 스크립트가 운영 중일 경우 해당 취약점에 노출 됩니다.
- ❖ 현재, 해당 취약점은 Linux/Unix 기반의 CGI+Bash 스크립트기반 어플리케이션만 해당하는 것으로 확인되었습니다.

## II. 취약점 상세 (3/3)

### 3. CVE-2014-6271 취약점 유무 확인 방법

- 다음과 같은 명령어를 사용하여 Bash Shell 사용 여부 및 Bash Shell 버전 확인이 가능합니다.

```
cat /etc/shells  
bash | grep Version
```

- 실제 취약점의 존재 유무는 다음 코드 실행을 통해 간단히 확인 가능합니다

```
env x='() { :; }; echo vulnerable' bash -c 'echo success'
```

#### ❖ 취약하지 않을 경우

```
bash: warning: x: ignoring function definition attempt  
bash: error importing function definition for `x'  
success
```

#### ❖ 취약할 경우

```
vulnerable  
success
```

### III. 대응 권고 방안 (1/5)

#### 1. 패치 방안

- 1) WAPPLES Bash Patch Toolkit 제공 예정입니다.
  - A. WAPPLES 영향도 분석 결과 취약점은 없으나, 필요 시 패치가 가능하도록 Toolkit 제공 예정
  - B. 제공일정 : ~10/03 이후 (내부검증기간에 따라 변경될 수 있음)

#### 2. Web Server 취약점 대응 방안

- 1) 영향을 받지 않는 Bash 버전으로 패치 할 것을 권고 합니다.
- 2) WAPPLES을 이용한 대응 권고 방안은 아래와 같습니다.
  - A. Web Server 영향도 분석에서 취약점이 존재하는 것으로 확인된 케이스에서 서비스가 운영되고 있을 경우, User Defined Pattern 등록으로 차단 대응이 가능합니다.
  - B. 추가적으로, Stealth Commanding 정책 설정을 통해서도 일부 대응이 가능합니다

### III. 대응 권고 방안 (2/5)

#### 3. 상세 설정 - User Defined Pattern 적용

- 1) 적용 가능 버전: v2.0R9 이상
- 2) 적용 방법 1: 패턴 저장소에 패턴 추가
  - A. 관리도구 접속
  - B. 설정 마법사 선택
  - C. 운영 설정 선택
  - D. 패턴저장소 선택
    - ① 패턴 추가 (※[D. 적용 패턴 리스트] 참고)

설정 마법사

패턴 저장소

패턴 추가

▶ 패턴을 추가합니다.

패턴 이름 :  
패턴

탐지 위치 :  
탐지 패턴 :  
Key :

TEST,PATTERN

REQLINE  
TEST,TEST

모두 탐지

탐지 위치

패턴

REQLINE

TEST,TEST

취소

다음 >

취약점 분석 보고서 | Penta Security Systems

SL5 PUBLIC



### III. 대응 권고 방안 (3/5)

#### 3. 상세 설정 - User Defined Pattern 적용

- 3) 적용 방법 2: User Defined Pattern 를 정책 설정
  - A. 관리도구 접속
  - B. 정책 설정 선택
  - C. 설정 수정이 필요한 정책을 선택 후 User Defined Pattern을 선택하여 사용자 정의 진행
  - D. 적용이 필요한 패턴 등록

User Defined Pattern

User Defined Pattern

패턴 저장소

이름	탐지패턴 수	Regex
----	--------	-------

패턴 적용

이름
TEST,PATTERN

>

<

확인

취소

### III. 대응 권고 방안 (4/5)

#### 3. 상세 설정 - User Defined Pattern 적용

##### 4) 적용 패턴 리스트

CVE-2014-6271

##### A. BASH\_CGI\_CVE-2014-6271

① 탐지위치 : REQLINE

② 탐지패턴 : .sh

(특정 확장자만 적용 하는 것을 권고, CGI경우 .cgi나 .sh를 이용)

**설정 마법사**

**패턴 저장소**  
패턴 수정

> 패턴을 수정합니다.

패턴 이름 :

패턴

탐지위치 :

탐지 패턴 :

Key :  ☐ 모두 탐지

탐지 위치	패턴
REQLINE	.sh

취소 다음 >

### III. 대응 권고 방안 (5/5)

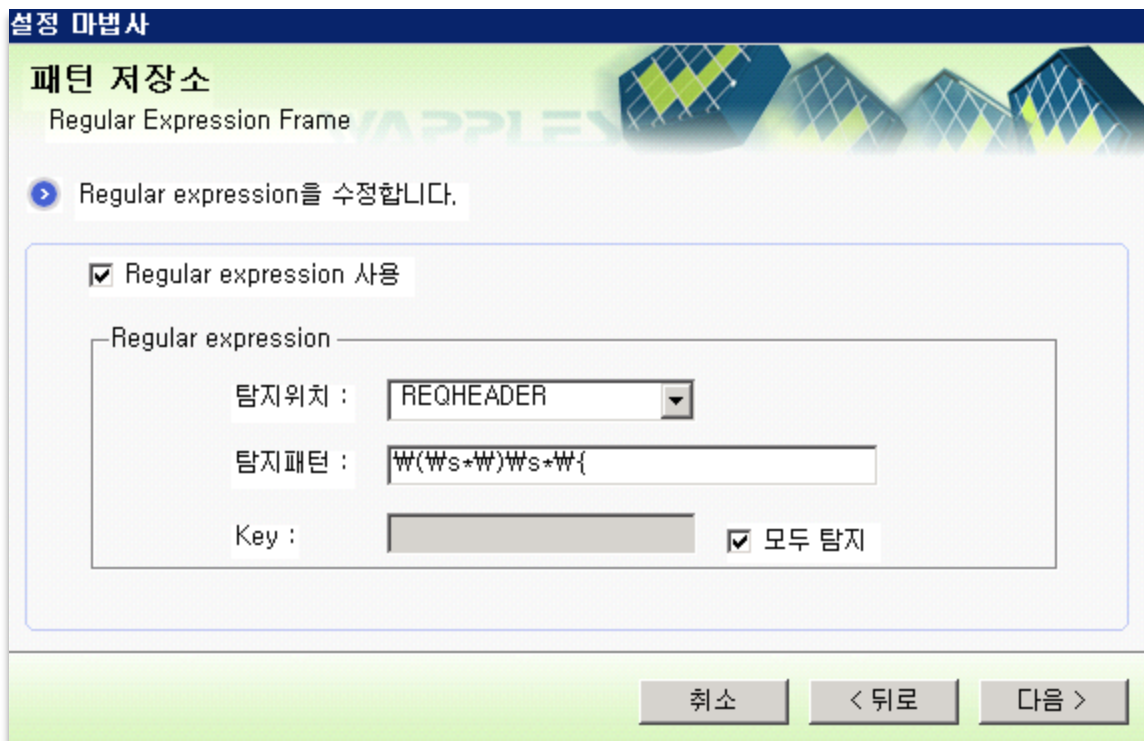
#### 3. 상세 설정 - User Defined Pattern 적용

##### 4) 적용 패턴 리스트

CVE-2014-6271

##### A. BASH\_CGI\_CVE-2014-6271

- ③ Regular expression 설정
  - a. 탐지위치 : REQHEADER
  - b. 탐지패턴 : `W(ws*W)Ws*W{`
  - c. Key : 모두 탐지



설정 마법사

### 패턴 저장소

Regular Expression Frame

> Regular expression을 수정합니다.

☒ Regular expression 사용

Regular expression

탐지위치 : REQHEADER

탐지패턴 : `W(ws*W)Ws*W{`

Key :  ☒ 모두 탐지

취소 < 뒤로 다음 >

t h a n k y o u



**Penta Security Systems Inc. (Headquarter)**

Hanjin Shipping Bldg. 20th fl. 25-11  
Yoido-dong, Youngdeungpo-ku, Seoul, Korea 150-949  
Tel. 82-2-780-7728 Fax. 82-2-786-5281 / [www.pentasecurity.com](http://www.pentasecurity.com)

**Penta Security Systems K.K. (Branch)**

Ascend Akasaka Bldg. 3F, 3-2-8 Akasaka,  
Minato-Ku, Tokyo 107-0052 Japan  
Tel. 81-3-5573-8191 Fax. 81-3-5573-8193 /  
[www.pentasecurity.co.jp](http://www.pentasecurity.co.jp)

Copyright 2013 Penta Security Systems Inc. All rights reserved.