
INetCop Security Advisory #2003-0x82-013

* Title: Kebi Academy 2001

Web Solution Directory Traversing Vulnerability.

0x01. Description

Kebi Academy 2001 is web solution that is supplied to C Binary CGI in web.

Fatal vulnerability that can read or can write,

and execute uploading malignancy code interior file of system in remote of this web solution exists.

Vulnerability happens because don't filter "../" from homepage file administration

contents of web solution. If exploit of vulnerability succeeds,

is possible to be writing with reading file as competence of webserver.

Also, result that attacker can execute shell in remote if upload malignancy code to directory that cgi or php file can be executed happens.

0x02. Vulnerable Packages

Vendor site: <http://solution.nara.co.kr/>

Kebi Academy 2001 Solution

+Linux

+Unix

* We already, liaised to vendor.

0x03. Exploit

Can read certain file as following as competence of webserver.

`http://target.com/k/home?dir=/&file=../../../../../../../../etc/passwd&lang=kor`

If become so, can get other user's database and so on which can get as competence of web server.

Also, can upload certain file to directory that competence of web server is permitted.

In case attacker uploads code that is enemy of evil,

it can enforce very fatal attack.

0x04. Patch

--

It can solve these problems as chroot() function.

Desire to compose safer web solution.

--

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>

--