

Hosting Controller's – Multiple Security Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-01/0041.html>

From: Phuong Nguyen (dphuong@yahoo.com)

Date: 01/05/02

Date: Sat, 5 Jan 2002 07:06:49 -0800 (PST)

From: Phuong Nguyen <dphuong@yahoo.com>

To: BugTraq <bugtraq@securityfocus.com>

Hosting Controller – Multiple security vulnerabilities

Release Date: 01/04/2002

Summary

Hosting Controller is an all in one administrative hosting tools for Windows. It automates all hosting tasks and gives full control of each website to the respective owners. Hosting Controller is used widely by many hosting providers.

More informations at <http://www.hostingcontroller.com>

Vulnerable version: 1.4.1 and probably all other versions

Vulnerability (1) – Directories Browsing

Hosting Controller has a security flaw which allows outside attackers to browse any file and any directory on that server without any authentication. You're not allowed to read files. However, I believe the second vulnerability (explained below) will allow you to take control of the server.

Example: Scripts that allow you to browse anywhere on the server.

<http://www.victim.com/advwebadmin/stats/statsbrowse.asp?filepath=c:\&Opt=3>

http://www.victim.com/advwedadmin/serv_u/servubrowse.asp?filepath=c:\&Opt=3

<http://www.victim.com/advwedadmin/adminsettings/browsedisk.asp?filepath=c:\&Opt=3>

SecurityFocus Bugtraq: Hosting Controller's – Multiple Security Vulnerabilities

<http://www.victim.com/advwedadmin/adminsettings/browsewebalizerexe.asp?filepath=c:\&Opt=3>

<http://www.victim.com/advwedadmin/SQLServ/sqlbrowse.asp?filepath=c:\&Opt=3>

advwedadmin is the path to hosting controller script,
replace advwebadmin with something else if necessary ,
for example /admin/ or /hostingcontroller/

Vulnerability (2) – Dot Dot Slash bug and
autosignup/dsp_newwebadmin.asp

The dsp_newwebadmin.asp script can be executed by
typing

www.victim.com/advwebadmin/autosignup/dsp_newwebadmin.asp
which allows you to create a new domain name and a new
account without the need of logging in as
administrator. Login to the hosting controller after
your account has been created by using the
dsp_newwebadmin.asp. Once you have logged in, you
should be able to use all of the options on the
hosting controller's menu as an owner of the account.
You will not be able to access the domain name you
just created with dsp_newwebadmin.asp because it needs
to be activated by the resadmin; so your domain name
should be inactive ;) (OBVIOUSLY) I'll explain how
you can gain control and execute code on that machine.

If you click on directories option on the left
handside, it will take you to file manager page and
you are only allowed to manage files within
<drive>:\webpace\resadmin\youraccount\youraccount.com
, but the filemanager.asp is also vulnerable, it's
vulnerable to the infamous dot dot slash bug /../
which allows directory traversal, so it should look
something like this

<http://www.victim.com/advwebadmin/folders/filemanager.aspg.comwebpace\resadmin\testing\testing.com\www\..\..\>

You'll have the ability to read, delete, rename file
and upload file anywhere you want. All you need to do
now is to upload something like ntdaddy.asp or
cmdasp.asp to some active domain names to be able
execute commands via web browser.
You can upload nc.exe and execute nc.exe by calling an
asp script from your browser. The possibilities are
endless.

Vendor has been contacted.

Do You Yahoo!?

Send FREE video emails in Yahoo! Mail!

<http://promo.yahoo.com/videomail/>

- *Previous message:* [Tamer Sahin: "Savant Webserver Buffer Overflow Vulnerability"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)