

[NT] Hosting Controller Multiple Security Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0027.html>

From: support@securiteam.com

Date: 01/08/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 8 Jan 2002 23:25:57 +0100 (CET)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Hosting Controller Multiple Security Vulnerabilities

SUMMARY

<<http://www.hostingcontroller.com/>> 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. Multiple security vulnerabilities in the product allow reading of any file, and gaining of administrative privileges.

DETAILS

Directories Browsing

Hosting Controller has a security flaw that allows outside attackers to browse any file and any directory on that server without any authentication. This vulnerability does not give access to the file content.

Example:

Scripts that allow you to browse anywhere on the server.

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

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

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

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

Securiteam: [NT] Hosting Controller Multiple Security Vulnerabilities

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

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

DotDot Slash bug and autosignup/dsp_newwebadmin.asp

The dsp_newwebadmin.asp script can be executed by typing:

www.example.com/advwebadmin/autosignup/dsp_newwebadmin.asp

That allows you to create a new domain name and a new account without the need of logging in as administrator. Log in 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, we will explain how you can gain control and execute code on that machine.

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

<http://www.example.com/advwebadmin/folders/filemanager.asp&sitename=testing.com&OpenPath=C:\webspaces\resadmin\testing\testing.com\www\..\..\..\..\>

You will 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 to execute commands via the web browser. You can upload nc.exe and execute nc.exe by calling an asp script from your browser. The possibilities are endless.

ADDITIONAL INFORMATION

The information has been provided by <mailto:dphuong@yahoo.com> Phuong Nguyen.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

Securiteam: [NT] Hosting Controller Multiple Security Vulnerabilities

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- **Previous message:** support@securiteam.com: "[NEWS] Cross Site Scripting Vulnerability in Microsoft.com"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)