

[NT] Multiple Information Disclosure In Hosting Controller (Log Disclosure, Admin E-Mail)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0023.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/09/05

To: list@securiteam.com

Date: 9 Mar 2005 10:45:41 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Multiple Information Disclosure In Hosting Controller (Log Disclosure, Admin E-Mail)

SUMMARY

<<http://www.hostingcontroller.com>> Hosting Controller is a complete hosting automation tool for Windows 2000 servers.

Hosting Controller contains multiple information disclosure vulnerabilities that allows an attacker to gain information about the computer array managed by Hosting Controller.

DETAILS

Vulnerable Systems:

*Hosting Controller version 6.1 Hotfix 1.7, prior versions may be vulnerable as well.

Log Discloser

The product includes a feature for a periodical log update update. This log is saved in a .CSV format and it's storage path is in web-root of server. This allows any user to access the logs and see saved information such as bandwidth report and disk usage report. As this is a full system

Securiteam: [NT] Multiple Information Disclosure In Hosting Controller (Log Disclosure, Admin E-Mail)

log, reports from all the hosted domains are also stored at the log file.

Proof Of Concept:

http://[target]/admin/logs/HCDiskQuotaService.csv

Admin E-Mail

There is a password recovery feature at the Admin login page of Hosting Controller, which send back the password to registered E-Mail address saved in the system. If you know the site domain name, it is possible to get this administrative email by submitting it in the login ID field the domain name without the top domain (.com/.net/etc.). Hosting Controller will disclose the hosting owners E-Mail.

Disclosure Timeline:

3/6/2005 Vendor Contacted.

3/8/2005 Release Date.

ADDITIONAL INFORMATION

The information has been provided by <mailto:small.mouse@gmail.com> small mouse.

The original article can be found at: <<http://isun.Shabgard.org/hc2.html>>
<http://isun.Shabgard.org/hc2.html>

=====

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

=====

=====

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.