

[UNIX] CuteNews Information Disclosure

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0002.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/01/03

To: list@securiteam.com

Date: 1 Dec 2003 13:02:23 +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>

CuteNews Information Disclosure

SUMMARY

<<http://cutephp.com/cutenews/index.php>> CuteNews is "a powerful and easy for using news management system that use flat files to store its database". A vulnerability in the product allows remote attacker to disclose sensitive information about the computer and enviroment the product is installed under.

DETAILS

Vulnerable systems:

- * CuteNews version 1.3
- * CuteNews version 1.2 and prior

Vulnerable code:

In the file `index.php`, a condition can be made to execute the PHP function `phpinfo()`; Here is the interesting lines:

```
if($HTTP_SERVER_VARS['QUERY_STRING'] == "debug"){ debug(); } ... function
debug(){
    global $config_version_name, $config_version_id,
    $config_http_script_dir;
    echo"<center><b>CuteNews Debug Information:</b><hr><br>";
```

Securiteam: [UNIX] CuteNews Information Disclosure

```
echo"Script Version/ID: $config_version_name / $config_version_id<br>";  
echo"\$config_http_script_dir: $config_http_script_dir<br><BR>";  
echo"<hr>";  
phpinfo();  
  
exit();  
}
```

Exploit:

By requesting a URL such as <http://victim.com/cutenews/index.php?debug>, the content of the phpinfo() function will be returned instead of the normal index page.

ADDITIONAL INFORMATION

The information has been provided by <mailto:webmaster@securiteinfo.com>
Arnaud Jacques aka scrap.

=====

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.