

[UNIX] CuteNews HTML Injection Vulnerability Via Commentaries

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0097.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/27/04

To: list@securiteam.com

Date: 27 Jul 2004 19:54:27 +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 HTML Injection Vulnerability Via Commentaries

SUMMARY

" <<http://cutephp.com/cutenews/>> CuteNews is a powerful and easy for using news management system that use flat files to store its database. It supports comments, archives, search function, image uploading, backup function, IP banning, flood protection and more..."

HTML code can be injected via the commentaries feature of CuteNews. The implication of this is that an attacker that maliciously injects HTML code for a victim to watch can get the code to execute by the victim, providing various degrees of risk.

DETAILS

Vulnerable Systems:

* CuteNews version 1.3.x

The commentaries feature of CuteNews is susceptible to an HTML injection that could endanger users of the system. In the "/inc/Shows.inc.php" file, line 189:

```
if(!$found){ fwrite($new_comments,
```

Securiteam: [UNIX] CuteNews HTML Injection Vulnerability Via Commentaries

```
"$id|>|$time|$name|$mail|$ip|$comments||\n"); }
```

The user-input variable \$id is not filtered and therefore anything can be passed through it. Since the commentaries are viewable by other users, HTML inserted as input through the use of \$id would cause HTML to be rendered by the user's browser viewing the commentary. An example follows:
show_news.php?subaction=addcomment&name=DarkBich0&comments=<http://www.darkbicho.tk&id=1078525267>>

The result of such an attack can be seen at
<<http://www.darkbicho.iberhosting.net/cutenews/cutenews.gif>>
<http://www.darkbicho.iberhosting.net/cutenews/cutenews.gif>.

An exploit is available at
<<http://www.darkbicho.iberhosting.net/cutenews/>>
<http://www.darkbicho.iberhosting.net/cutenews/>.

Vendor Status:

Vendors were contacted many weeks ago and plan to release a fixed version soon. Check the CuteNews website for updates and official release details.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:darkbicho@fastmail.fm>>
DarkBicho.

=====

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.