

[UNIX] CuteNews Code Execution (ip2long)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0101.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/27/05

To: list@securiteam.com

Date: 27 Sep 2005 15:44:38 +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 Code Execution (ip2long)

SUMMARY

" <<http://cutephp.com/>> Cute news 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..."

Lack of proper parameter filtering and validation allows attackers to execute arbitrary code in CuteNews.

DETAILS

Vulnerable Systems:

* CuteNews version 1.4.0

CuteNews uses the environment variable HTTP_CLIENT_IP and the PHP function ip2long. The function ip2long always return true regardless of the content that should be an IP address. CuteNews does not validate that the IP address is valid and only care for the result of the ip2long function.

Vulnerable Code:

```
..  
//-----
```

Securiteam: [UNIX] CuteNews Code Execution (ip2long)

```
// Get the IP
//-----
$foundip = TRUE;
[!] if (getenv("HTTP_CLIENT_IP")) $ip = getenv("HTTP_CLIENT_IP");
    [!]
    else if(getenv("REMOTE_ADDR")) $ip = getenv("REMOTE_ADDR");
    else if(getenv("HTTP_X_FORWARDED_FOR")) $ip =
getenv("HTTP_X_FORWARDED_FOR");
    else {$ip = "not detected"; $foundip = FALSE;}
[!] if( $foundip and !ip2long($ip) ){ $ip = "not detected"; $foundip =
FALSE;} //ensure that what we have is a real IP [!]
..
```

By crafting a special IP address in the HTTP request it is possible to inject arbitrary code and cause CuteNews to execute it.

ADDITIONAL INFORMATION

The information has been provided by <mailto:retrogod@aliceposta.it>
rgod.

The exploit can be found at:

<<http://www.securiteam.com/exploits/5KP0D2KGUI.html>>

<http://www.securiteam.com/exploits/5KP0D2KGUI.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.