

[UNIX] XOOPS Weak File Validation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0107.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/23/05

To: list@securiteam.com

Date: 23 Mar 2005 10:15:10 +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>

XOOPS Weak File Validation

SUMMARY

<<http://www.xoops.org/>> XOOPS is an extensible, OO (Object Oriented), easy to use dynamic web content management system written in PHP.

XOOPS does not check if a content of an uploaded file of avatars is a valid image, this allows an attacker to upload malicious script files which in turn can be used to preform malicious acts.

DETAILS

Vulnerable Systems:

- * XOOPS version 2.0.9.2 and prior

User may upload malicious files containing arbitrary commands posed as images through the avatar uploading mechanism if "Allow custom avatar upload" is set to "Yes" in "User Info Settings" (the setting is not 'Yes' by default).

This is due to weak file extension validation of the XoopsMediaUploader class in file uploader.php, which doesn't check for all the possible extensions malicious files can come as:

```
if ( preg_match( '\.(php|cgi|pl|py|asp)$/' , $this->mediaName ) )
```

Securiteam: [UNIX] XOOPS Weak File Validation

```
{  
  $this->setErrors('Filename rejected');  
  return false;  
}
```

Workaround:

Set "Allow custom avatar upload" to "No" in "User Info Settings".

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:pokleyzz@scan-associates.net>> pokley .

=====

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.