Security Bulletin: TURN OFF CUSTOM AVATAR UPLOAD - Security

NEWS_PDF_AUTHOR: Mithrandir

NEWS_PDF_DATE: 2005/3/8 7:30:00

A vulnerability has been reported in the XOOPS core that allows registered users to upload possibly malicious scripts to the webserver.

The vulnerability is in the upload of custom avatars and until we have complete overview of the consequences and correction of this exploit, we advise all XOOPS site administrators to TURN OFF CUSTOM AVATAR UPLOAD in System Admin -> Preferences -> User Info Settings -> "Allow Custom Avatar Upload"

ALSO, do NOT allow any non-trusted users to upload images through the image manager. i.e. in Administration Menu -> System Admin -> Images edit each and every category to NOT allow uploading by non-trusted usergroups.

We will keep you informed as soon as we have a fix for this exploit.

XOOPS Core Development Team

UPDATE:
A fix is available.
If no specific problem is encountered after deeper tests, it will be released tomorrow.

In the meantime, people you would like to try it and give us some feedback are welcome.
To install it, upload the two following files to your XOOPS /class/ folder:
uploader.php (check that you get the revision 1.18 or wait a little...)
mimetypes.inc.php

The SF viewcvs updates are made regularly, but you may have to wait a few more minutes before the files become available. Alternatively, people with anonymous cvs access can get them from the XOOPS cvs repository right now.

skalpa.>
(with the appreciated help of php_pp :)

A vulnerability has been reported in the XOOPS core that allows registered users to upload possibly malicious scripts to the webserver.

The vulnerability is in the upload of custom avatars and until we have complete overview of the consequences and correction of this exploit, we advise all XOOPS site administrators to TURN OFF CUSTOM AVATAR UPLOAD in System Admin -> Preferences -> User Info Settings -> "Allow Custom Avatar Upload"

ALSO, do NOT allow any non-trusted users to upload images through the image manager. i.e. in Administration Menu -> System Admin -> Images edit each and every category to NOT allow uploading by non-trusted usergroups.

We will keep you informed as soon as we have a fix for this exploit.

XOOPS Core Development Team

UPDATE:
A fix is available.
If no specific problem is encountered after deeper tests, it will be released tomorrow.

In the meantime, people you would like to try it and give us some feedback are welcome.
To install it, upload the two following files to your XOOPS /class/ folder:
uploader.php (check that you get the revision 1.18 or wait a little...)
mimetypes.inc.php

The SF viewcvs updates are made regularly, but you may have to wait a few more minutes before the files become available. Alternatively, people with anonymous cvs access can get them from the XOOPS cvs repository right now.

skalpa.>
(with the appreciated help of php_pp :)