Directory traversal vulnerability on Xoops CMS module "tutorials" - Security

NEWS_PDF_AUTHOR: ac3__

NEWS_PDF_DATE: 2003/6/15 14:42:46

Short description:

An attacker can use this flaw to execute arbitrary code of his choice on the remote system, run with the privileges of httpd. The code can be written in any scripting language whose parser is run in the remote system in cooporation with httpd, whether as module or executable.

Details:

This vulnerability affects systems where Xoops or E-Xoops PHP CMS is installed, along with it's "Tutorials 2.0" module. Tutorials module normally allows users to submit HTML/BBcode formatted content to a site. Uploading of local image files is supported through php embedded uploader. It is however possible for a user to use this uploader to upload files of no image MIME type (e.x. PHP scripts), and then execute them by sending a simple http request. Retrieval or even deletion of sensitive System files on the remote machine may be possible this way, depending on the privileges under which the httpd is running and the configuration of PHP parser!

Best solution: Update to version 2.1 in which the PHP uploader has included a MIME filetype check, prior to uploading.

Other Possible Solutions: change the permissions to the /images/ directory to 555

Tested on Xoops 1.3.10

Update available: Yes, at http://www.mytutorials.info/modules/mydownloads

Credits
ac3 (ac3@security-lab.org)
GUSG Team
http://www.hack-box.com,
http://www.security-lab.org
with regards to Violator for testing.

Short description:

An attacker can use this flaw to execute arbitrary code of his choice on the remote system, run with the privileges of httpd. The code can be written in any scripting language whose parser is run in the remote system in cooporation with httpd, whether as module or executable.

Details:

This vulnerability affects systems where Xoops or E-Xoops PHP CMS is installed, along with it's "Tutorials 2.0" module. Tutorials module normally allows users to submit HTML/BBcode formatted content to a site. Uploading of local image files is supported through php embedded uploader. It is however possible for a user to use this uploader to upload files of no image MIME type (e.x. PHP scripts), and then execute them by sending a simple http request. Retrieval or even deletion of sensitive System files on the remote machine may be possible this way, depending on the privileges under which the httpd is running and the configuration of PHP parser!

Best solution: Update to version 2.1 in which the PHP uploader has included a MIME filetype check, prior to uploading.

Other Possible Solutions: change the permissions to the /images/ directory to 555

Tested on Xoops 1.3.10

Update available: Yes, at http://www.mytutorials.info/modules/mydownloads

Credits
ac3 (ac3@security-lab.org)
GUSG Team
http://www.hack-box.com,
http://www.security-lab.org
with regards to Violator for testing.