

Name: PHP-nuke web portal system
Vendor URL: http://www.phpnuke.org
Author: Karol Więsek <appelast@drumnbass.art.pl>

Issue:

Remote attacker could transfer to server his own file or copy arbitrary file from system to accessible directory.

Details:

Remote attacker could transfer to server his own file or copy arbitrary file from system to accessible directory. The result of such acts could be remote execution commands under privileges of http server, or retrieving important information such as database login and password. Attacker don't have to be registered user to make an attack.

The crux of the problem lies in WebMail module, and exactly in mailattach.php file. This Module is default attached to PHP-nuke 6.0 (current). And even this module does not have to be active to make an attack successful, because it can be accessed directly (no modules.php in \$PHP_SELF check present in this file).

mailatach.php

```
if (isset($userfile) AND $userfile != "none") {  
    if (ini_get(file_uploads) AND $attachments == 1) {  
        $updir = "tmp";  
        @copy($userfile, "$updir/$userfile_name");  
        @unlink($userfile);  
    }  
}
```

Sample attack which allows an attacker to grab database password and login.

http://target.server/modules/WebMail/mailattach.php?userfile=../../config.php&userfile_name=../../attachments/file.txt&attachments=1

Using mailattach.php attacker could upload file with any extension, which allow him to upload any .php file and execute arbitrary PHP code.

To successfully exploiting this vulnerability writable directory is needed. When module is active, the tmp and attachments should be writable to allow module work properly.

PHP-nuke with WebMail 0.9.3 is confirmed vulnerable.