

[UNIX] Mantis Bug Tracker Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0072.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/22/04

To: list@securiteam.com

Date: 22 Aug 2004 17:24:17 +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>

Mantis Bug Tracker Multiple Vulnerabilities

SUMMARY

<<http://www.mantisbt.org/>> Mantis is "a web-based bug tracking system. It is written in the PHP scripting language and requires the MySQL database and a web server".

The Mantis bug tracking system suffers from multiple security issues mainly due to improper input validation. Hence, cross-site scripting and even PHP code execution are possible through this system.

DETAILS

Vulnerable Systems:

- * Mantis version 0.18.3

Immune Systems:

- * Mantis version 0.19.0a2 (Alpha) from CVS

* The 'return' parameter in the login_page.php script are not properly sanitized and allow a malicious user to input malicious content. It is possible to login anonymously and in order to perform a privileged action, login as a registered user. The previous URL is passed as the return parameter and through it, any HTML or script code can be injected. An

Securiteam: [UNIX] Mantis Bug Tracker Multiple Vulnerabilities

```
echo("URL is $url\n");
$fd = fopen($url,"r");
echo("E-mail $i sended\n");
fclose($fd);
}
```

?>

Finally, there is also a remote PHP code execution in the system. If the REGISTER_GLOBAL variable is set, an attacker is able to inject and execute PHP code by overwriting the \$_core_dir global variable. The vulnerable scripts are:

bug_api.php -> at line 22 (using variable \$_core_path)

relationship_api.php -> Line 14 (using variable \$_core_dir)

Vendor Status:

The maintainers of Mantis have been informed and the fixes are already in the CVS tree, in the alpha version.

ADDITIONAL INFORMATION

The information has been provided by <mailto:joxeankoret@yahoo.es> Joxean Koret.

=====

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.