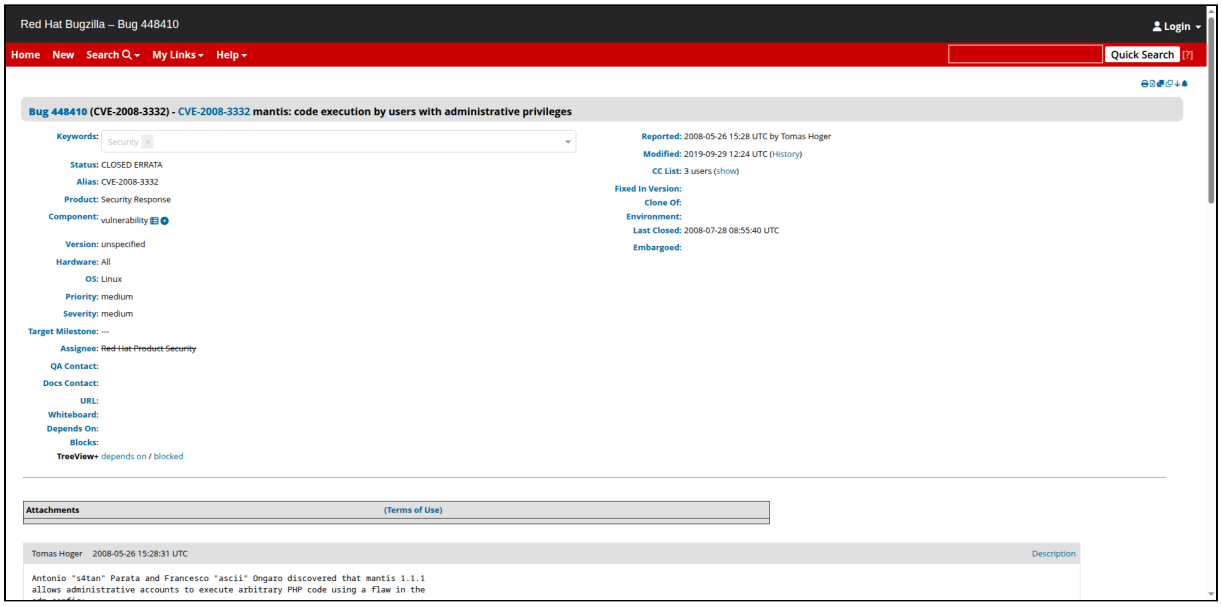
PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

Page Screenshot



Bug 448410 (CVE-2008-3332) - CVE-2008-3332 mantis: code execution by users with administrative privileges

Keywords: Security

Status: CLOSED ERRATA

Alias: CVE-2008-3332

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: ~~Red Hat Product Security~~

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2008-05-26 15:28 UTC by Tomas Hoger

Modified: 2019-09-29 12:24 UTC (History)

CC List: 3 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed: 2008-07-28 08:55:40 UTC

Embargoed:

Attachments (Terms of Use)

Tomas Hoger 2008-05-26 15:28:31 UTC Description

```
Antonio "s4tan" Parata and Francesco "ascii" Ongaro discovered that mantis 1.1.1
allows administrative accounts to execute arbitrary PHP code using a flaw in the
adm_config:

  C) Remote Code Execution Vulnerabilities

  Finally we present the most critical vulnerability. A Remote Code
  Execution vulnerability exists in the software, but it can be exploited
  only if the attacker has a valid administrator account, so it could be
  ideal if used in conjunction with the previous one. The vulnerability
  is in the file adm_config_set.php. On row 80 we have the following
  statement:

  eval( '$t_value = ' . $f_value . ';' );

  where the $f_value is defined at row 34 of the same file:

  $f_value = gpc_get_string( 'value' );

  the parameter $f_value is never validated, so we can exploit this issue
  with the following url which executes the phpinfo() function:

  http://www.example.com/mantis/adm_config_set.php?user_id=0&project_id=0
  &config_option=cache_config&type=0&value=0;phpinfo()

References:
http://marc.info/?l=bugtraq&m=121130774617956&w=4
http://www.ush.it/team/ush/hack-mantis111/adv.txt

Upstream bug reports (currently restricted):
http://www.mantisbt.org/bugs/view.php?id=8976
http://www.mantisbt.org/bugs/view.php?id=8980

Upstream commit in 1.1 SVN branch:
http://mantisbt.svn.sourceforge.net/viewvc/mantisbt?view=rev&revision=5121
(partial fix according to the commit message)

This is probably not an issue in situations when all admin mantis users are
expected to be able to execute own PHP scripts on the host with the privileges
of web server (e.g. when they also have normal user account and web server
configured to serve content of public_html directories).
```

Fedora Update System 2008-07-19 22:10:56 UTC Comment 1

mantis-1.1.2-1.fc9 has been submitted as an update for Fedora 9

Fedora Update System 2008-07-19 22:14:39 UTC Comment 2

mantis-1.1.2-1.fc8 has been submitted as an update for Fedora 8

Fedora Update System 2008-07-23 07:20:07 UTC Comment 3

mantis-1.1.2-1.fc9 has been pushed to the Fedora 9 stable repository. If problems still persist, please make note of it in this bug report.

Fedora Update System 2008-07-23 07:21:37 UTC Comment 4

mantis-1.1.2-1.fc8 has been pushed to the Fedora 8 stable repository. If problems still persist, please make note of it in this bug report.

Tomas Hoger 2008-07-28 08:53:58 UTC Comment 5

CVE-2008-3332:
Eval injection vulnerability in adm_config_set.php in Mantis before 1.1.2 allows remote authenticated administrators to execute arbitrary code via the value parameter.

~~Red Hat Product Security~~ 2008-07-28 08:55:40 UTC Comment 6

This issue was addressed in:

Fedora:
https://admin.fedoraproject.org/updates/F8/FEDORA-2008-6657
https://admin.fedoraproject.org/updates/F9/FEDORA-2008-6647

Note

You need to log in before you can comment on or make changes to this bug.