

[UNIX] Remote Database Password Disclosure in Bugzilla

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0005.html>

From: support@securiteam.com

Date: 01/05/03

From: support@securiteam.com

To: list@securiteam.com

Date: 5 Jan 2003 10:57:49 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Remote Database Password Disclosure in Bugzilla

SUMMARY

All Bugzilla installations are advised to upgrade to the latest versions of Bugzilla, 2.14.5 and 2.16.2, both released today. Security issues of varying importance have been fixed in both branches. These vulnerabilities affect all previous 2.14 and 2.16 releases.

Development snapshots prior to version 2.17.3 are also affected, so if you are using a development snapshot, you should obtain a newer one or use CVS to update.

2.14.x users are additionally encouraged to upgrade to 2.16.2 as soon as possible, as this is the last 2.14.x release and the 2.14 branch will no longer be supported by the Bugzilla team.

This advisory covers two security bugs: one involves incorrect local permissions on a directory, allowing local users' access. The other involves protecting configuration information leaks due to backup files created by editors.

DETAILS

Securiteam: [UNIX] Remote Database Password Disclosure in Bugzilla

The following security issues were fixed in 2.14.5, 2.16.2, and 2.17.3:

- The provided data collection script intended to be run as a nightly cron job changes the permissions of the data/mining directory to be world-writable every time it runs. This would enable local users to alter or delete the collected data. (Bugzilla bug 183188 / Bugtraq ID 6502).
- The default .htaccess scripts provided by checksetup.pl do not block access to backups of the localconfig file that might be created by editors such as vi or emacs (typically these will have a .swp or ~suffix). This allows an end user to download one of the backup copies and potentially obtain your database password. If you already have such an editor backup in your bugzilla directory it would be advisable to change your database password in addition to upgrading.

In addition, we also continue to recommend hardening access to the Bugzilla database user account by limiting access to the account to the machine Bugzilla is served from (typically localhost); consult the MySQL documentation for more information on how to accomplish this. (Bugzilla bug 186383 / Bugtraq ID 6501)

Also included in these releases are the patches that were posted as part of our earlier security advisory on November 26th, 2002. (Bugzilla bug 179329)

Vulnerability Solutions:

The fixes for both security bugs contained in this release, as well as the previously announced security bug involving cross-site scripting vulnerabilities are contained in the 2.14.5, 2.16.2, and 2.17.3 releases. Upgrading to these releases will protect installations against exploitations of these security bugs.

Individual patches to upgrade Bugzilla are available at:

<<http://ftp.mozilla.org/pub/webtools/>>

<http://ftp.mozilla.org/pub/webtools/> (these patches are only valid for 2.14.4 and 2.16.1 users).

Full release downloads and CVS upgrade instructions are available at

<<http://www.bugzilla.org/download.html>>

<http://www.bugzilla.org/download.html>

References:

Complete bug reports for the security bugs covered herein may be obtained at:

<http://bugzilla.mozilla.org/show_bug.cgi?id=183188>

http://bugzilla.mozilla.org/show_bug.cgi?id=183188

<http://bugzilla.mozilla.org/show_bug.cgi?id=186383>

http://bugzilla.mozilla.org/show_bug.cgi?id=186383

General information about the Bugzilla bug-tracking system can be found at

<<http://www.bugzilla.org/>> <http://www.bugzilla.org/>

Securiteam: [UNIX] Remote Database Password Disclosure in Bugzilla

Comments and follow-ups can be directed to the netscape.public.mozilla.webtools newsgroup or the mozilla-webtools mailing list; <<http://www.mozilla.org/community.html>> <http://www.mozilla.org/community.html> has directions for accessing these forums.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:justdave@syndicomm.com>> David Miller.

=====

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.