

# [NEWS] Security Update for Bugzilla v2.13 and Older

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-09/0003.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 09/02/01

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Subject: [NEWS] Security Update for Bugzilla v2.13 and Older

Message-Id: <20010901222139.9B7AB138BF@mail.der-keiler.de>

Date: Sun, 2 Sep 2001 00:21:39 +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.

-----

Security Update for Bugzilla v2.13 and Older

---

## SUMMARY

All users of Bugzilla, the bug-tracking system from mozilla.org, are strongly recommended to update to version 2.14.

Bugzilla 2.14 is a general security update, but not all of the security issues are serious.

Serious issues include:

- \* Multiple instances where data on "confidential" bugs could be obtained by valid users of the system who are not authorized to do so.

- \* Multiple instances of security holes where parameters were not being checked/escaped properly.

Many patches need to be applied to properly close these holes. If you will not be upgrading your system to 2.14 and instead wish to apply these patches to your existing system, please consult the bug reports on [bugzilla.mozilla.org](http://bugzilla.mozilla.org) for the bug numbers listed below, where you can obtain the patches attached to those bugs.

## DETAILS

Complete bug reports for all bugs can be obtained by visiting the following URL: [http://bugzilla.mozilla.org/show\\_bug.cgi?id=XXXXXX](http://bugzilla.mozilla.org/show_bug.cgi?id=XXXXXX) where you replace the XXXXX at the end of the URL with a bug number as listed below. You may also enter the bug numbers in the "enter a bug#" box on the main page at <http://bugzilla.mozilla.org/> or in the footer of any other page on bugzilla.mozilla.org.

\*\*\* SECURITY ISSUES RESOLVED \*\*\*

– Multiple instances of unauthorized access to confidential bugs have been fixed.

(bug 39524, 39526, 39527, 39531, 39533, 70189, and 82781)

– Multiple instances of untrusted parameters not being checked/escaped were fixed. These included definite security holes.

(bug 38854, 38855, 38859, 39536, 87701, and 95235)

– After logging in passwords no longer appear in the URL.

(bug 15980)

– Procedures to prevent unauthorized access to confidential files are now simpler. In particular the shadow directory no longer exists and the data/comments file no longer needs to be directly accessible, so the entire data directory can be blocked. However, no changes are required here if you have a properly secured 2.12 installation as no new files must be protected.

(bug 71552, 73191)

– If they do not already exist, checksetup.pl will attempt to write Apache htaccess files by default, to prevent unauthorized access to confidential files. You can turn this off in the localconfig file.

(bug 76154)

– Sanity check can now only be run by people in the 'editbugs' group. Although it would be better to have a separate group, this is not possible until the limitation on the number of groups allowed has been removed.

(bug 54556)

– The password is no longer stored in plaintext form. It will be eradicated next time you run checksetup.pl. A user must now change their password via a password change request that is validated at their e-mail account, rather than have it mailed to them.

(bug 74032)

– When you using product groups and you move a bug between products (single or mass change), the bug will no longer be restricted to the old product's group (if it was) and will be restricted to the new product's group.

(bug 66235)

– There are now options on a bug to choose whether the reporter, assignee, QA, and CCs can access a bug even if they are not in groups the bug it is restricted to.

(bug 39816)

– You can no longer mark a bug as a duplicate of a bug you can't see, and if you mark a bug a duplicate of a bug the reporter cannot see you will be given options as to what to do regarding adding the reporter of the

Securiteam: [NEWS] Security Update for Bugzilla v2.13 and Older

resolved bug to the CC of the open bug.  
(bug 96085)

General information about the Bugzilla bug-tracking system can be found at  
<<http://www.mozilla.org/projects/bugzilla/>>  
<http://www.mozilla.org/projects/bugzilla/>

Comments and follow-ups can be directed to the  
netscape.public.mozilla.webtools newsgroup or the mozilla-webtools mailing  
list (see <<http://www.mozilla.org/community.html>>  
<http://www.mozilla.org/community.html> for directions how to access 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](mailto:list-unsubscribe@securiteam.com)  
In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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](mailto:support@securiteam.com): "[\[UNIX\] Easy Remote Detection of a Running Tripwire for Webpages System](#)"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)