

# [UNIX] Bugzilla Unauthorized Bug Modification And Information Disclosure Vulnerabilities

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0086.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 10/26/04

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

Date: 26 Oct 2004 17:42:57 +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>

-----  
Bugzilla Unauthorized Bug Modification And Information Disclosure  
Vulnerabilities  
-----

## SUMMARY

<<http://www.bugzilla.org/>> Bugzilla is a web-based bug (and enhancement) tracking engine built over MySQL. It's often used for distributed Open Source development, but is used by corporations (both internally and externally) as well.

Three security bugs have been found in Bugzilla and are documented in this advisory. The vulnerabilities range from private information disclosure to unauthorized bug modifications possible by a third party.

## DETAILS

Vulnerable Systems:

- \* Bugzilla version 2.16 stable (bug modification only)
- \* Bugzilla version 2.18 release candidates (RCs, information leaks)

Immune Systems:

- \* Bugzilla versions 2.16.7 and 2.18rc3

## Securiteam: [UNIX] Bugzilla Unauthorized Bug Modification And Information Disclosure Vulnerabilities

### Unauthorized Bug Modification

It is possible to send a carefully crafted HTTP POST message to process\_bug.cgi which will remove keywords from a bug even if you don't have permissions to edit all bug fields (the "editbugs" permission). Such changes are reported in "bug changed" email notifications, so they are easily detected and reversed if someone abuses it.

Reference:

<[https://bugzilla.mozilla.org/show\\_bug.cgi?id=252638](https://bugzilla.mozilla.org/show_bug.cgi?id=252638)>  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=252638](https://bugzilla.mozilla.org/show_bug.cgi?id=252638)

### Private User Comments and Attachment Summaries Leak In XML Bug Export

Exporting a bug to XML exposes user comments and attachment summaries which are marked as private to users who are not members of the group allowed to see private comments and attachments. XML export is not exposed in the user interface, but is available to anyone who knows the correct URL to invoke it. This only affects sites that use the 'insidergroup' feature.

Reference:

<[https://bugzilla.mozilla.org/show\\_bug.cgi?id=263780](https://bugzilla.mozilla.org/show_bug.cgi?id=263780)>  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=263780](https://bugzilla.mozilla.org/show_bug.cgi?id=263780)

### Private Metadata Changes For Attachments Information Leak

Changes to the metadata (filename, description, mime type, review flags) on attachments which were flagged as private get displayed to users who are not members of the group allowed to see private attachments when viewing the bug activity log and when receiving bug change notification mails. This only affects sites that use the 'insidergroup' feature.

References:

<[https://bugzilla.mozilla.org/show\\_bug.cgi?id=250605](https://bugzilla.mozilla.org/show_bug.cgi?id=250605)>  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=250605](https://bugzilla.mozilla.org/show_bug.cgi?id=250605)  
<[https://bugzilla.mozilla.org/show\\_bug.cgi?id=253544](https://bugzilla.mozilla.org/show_bug.cgi?id=253544)>  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=253544](https://bugzilla.mozilla.org/show_bug.cgi?id=253544)

### Patch Availability:

Fixes for all security bugs mentioned in this advisory are included in the 2.16.7 and 2.18rc3 releases, and in the 2.19.1 development snapshot. Upgrading to these releases will protect installations from possible exploits of these issues.

Full release downloads, patches to upgrade Bugzilla to 2.16.7 from previous 2.16.x versions, and CVS upgrade instructions are available at:

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

Specific patches for each of the individual issues can be found on the corresponding bug reports for each issue, at the URL given in the reference for that issue in the list above.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:justdave@bugzilla.org>> 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.