

[UNIX] Bugzilla Multiple Vulnerabilities (Unauthorized Bug Change, Information Disclosure)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0002.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/01/05

To: list@securiteam.com

Date: 1 Aug 2005 18:53:03 +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 Multiple Vulnerabilities (Unauthorized Bug Change, Information
Disclosure)

SUMMARY

<<http://www.bugzilla.org>> Bugzilla is "server software designed to help you manage software development".

Lack of proper privileges checking in Bugzilla, allows attackers to expose or hide bugs, change their status, and/or obtain bug information before changing their status to private.

DETAILS

Vulnerable Systems:

- * Bugzilla development snapshots version 2.19.3
- * Bugzilla version 2.18.1
- * Bugzilla version 2.17.1

Immune Systems:

- * Bugzilla version 2.18.2
- * Bugzilla version 2.20rc1

Securiteam: [UNIX] Bugzilla Multiple Vulnerabilities (Unauthorized Bug Change, Information Disclosure)

Unauthorized Bug Change:

Any user can change any flag on any bug, even if they don't have access to that bug, or even if they can't normally make bug changes. This also allows them to expose the summary of a bug.

By manually modifying a link to process_bug.cgi, it is possible to change a flag on a bug that you do not have access to, because Bugzilla does not validate that the flag you are attempting to change is associated with the bug that you are attempting to change.

If the attacker makes a flag change which causes the attacker to be emailed, the attacker will see the summary of the bug in that email.

If you are using the request_group or grant_group features of 2.19, the attacker will be prevented from exploiting this security hole if they do not have permission to change the flag in the fashion that they are changing it.

Information Disclosure:

Bugs are inserted into the database before they are marked as private, in Bugzilla code. Thus, MySQL replication can lag in between the time that the bug is inserted and when it is marked as private (usually less than a second). If replication lags at this point, the bug summary will be accessible to all users until replication catches up.

Also, on a very slow machine, there may be a pause longer than a second that allows users to see the title of the newly-filed bug.

Vendor Status:

The fixes for all of the security bugs mentioned in this advisory are included in the 2.18.2 and 2.20rc1 releases. Upgrading to these releases will protect installations from possible exploits of these issues.

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

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

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

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:mkanat@bugzilla.org> mkanat.

Bug reports about the issues can be found at:

<https://bugzilla.mozilla.org/show_bug.cgi?id=293159>

https://bugzilla.mozilla.org/show_bug.cgi?id=293159,

<https://bugzilla.mozilla.org/show_bug.cgi?id=292544>

https://bugzilla.mozilla.org/show_bug.cgi?id=292544

Securiteam: [UNIX] Bugzilla Multiple Vulnerabilities (Unauthorized Bug Change, Information Disclosure)

=====

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.