

[UNIX] Bugzilla Multiple Vulnerabilities (SQL Injections, Privileges Escalation, Information Leak)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0029.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/05/03

To: list@securiteam.com

Date: 5 Nov 2003 17:47:11 +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 (SQL Injections, Privileges Escalation, Information Leak)

SUMMARY

Bugzilla is a Web-based bug-tracking system, currently used by a large number of software projects.

This advisory covers security bugs that have recently been discovered and fixed in the Bugzilla code: two instances of arbitrary SQL injection exploitable only by a privileged user, one instance where a privileged user may retain privileges that should have been removed, and two instances of unprivileged access to summaries of restricted data.

These bugs are not considered critical, since their impact is quite limited. Nevertheless, all Bugzilla installations are advised to upgrade to the latest stable version of Bugzilla, 2.16.4, which was released today.

Development snapshots prior to version 2.17.5 are also affected, so if you are using a development snapshot, you should obtain a newer one (2.17.5) or use CVS to update.

DETAILS

Issue 1:

Class: SQL injection (by privileged user only)

Versions: 2.16.3 and earlier (2.17.1 and up are not affected)

Description: A user with 'editproducts' privileges (i.e. usually an administrator) can select arbitrary SQL to be run by the nightly statistics cron job (collectstats.pl), by giving a product a special name.

Reference: <http://bugzilla.mozilla.org/show_bug.cgi?id=214290>
http://bugzilla.mozilla.org/show_bug.cgi?id=214290

Issue 2:

Class: SQL injection (by privileged user only)

Versions: 2.16.3 and earlier, 2.17.1 through 2.17.4

Description: A user with 'editkeywords' privileges (i.e. usually an administrator) can inject arbitrary SQL via the URL used to edit an existing keyword.

Reference: <http://bugzilla.mozilla.org/show_bug.cgi?id=219044>
http://bugzilla.mozilla.org/show_bug.cgi?id=219044

Issue 3:

Class: Privilege mishandling

Versions: 2.16.3 and earlier (2.17.1 and up are not affected)

Description: When deleting products and the 'usebuggroups' parameter is on, the privilege which allows someone to add people to the group which is being deleted does not get removed, allowing people with that privilege to get that privilege for the next group that is created which reuses that group ID. Note that this only allows someone who had been granted privileges in the past to retain them.

Reference: <http://bugzilla.mozilla.org/show_bug.cgi?id=219690>
http://bugzilla.mozilla.org/show_bug.cgi?id=219690

Issue 4:

Class: Information leak

Versions: 2.16.3 and earlier, 2.17.1 through 2.17.4

Description: If you know the email address of someone who has voted on a secure bug, you can access the summary of that bug even if you do not have sufficient permissions to view the bug itself.

Reference: <http://bugzilla.mozilla.org/show_bug.cgi?id=209376>
http://bugzilla.mozilla.org/show_bug.cgi?id=209376

Issue 5:

Class: Information leak

Versions: 2.17.3 and 2.17.4 only

Description: Under some circumstances, a user can obtain component descriptions for a product to which he does not normally have access.

Reference: <http://bugzilla.mozilla.org/show_bug.cgi?id=209742>
http://bugzilla.mozilla.org/show_bug.cgi?id=209742

Vulnerability Solutions:

The fixes for all of the security bugs mentioned in this advisory are

Securiteam: [UNIX] Bugzilla Multiple Vulnerabilities (SQL Injections, Privileges Escalation, Information Leak)

included in the 2.16.4 and 2.17.5 releases. Upgrading to these releases will protect installations from these issues.

Full release downloads, patches to upgrade Bugzilla to 2.16.4 from previous 2.16.x versions, and CVS upgrade instructions are available at: <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: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.