

[UNIX] Call-Center-Software Multiple Security Issues

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-10/msg00049.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 12 Oct 2006 16:52:06 +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>

Call-Center-Software Multiple Security Issues

SUMMARY

<<http://www.call-center-software.org/>> Call-Center-Software is 'a free open-source application released under the GPL'. Call-Center-Software is vulnerable to multiple SQL injection attacks and XSS under certain conditions, along with privilege escalation.

DETAILS

XSS:

Call-Center-Software does not escape data when handling it allowing malicious javascript data to be inserted by any user. This is only when Magic Quotes is disabled within PHP.

Example:

A user entering <script>alert("Moo!");</script> into the problem description field when submitting the problem, will cause the javascript to be executed upon viewing or editing the problem.

SQL Injection:

Call-Center-Software does not escape data when handling it allowing

[UNIX] Call-Center-Software Multiple Security Issues

malicious users to inject SQL commands into the database. This is only when Magic Quotes is disabled within PHP.

Example:

By logging into the system with the user "'or 1=1 or 1='" the attacker is let into the system with full administrative privileges.

Privilege Escalation and Password Disclosure:

Call-Center-Software does not check access privileges when bringing up the "edit user" screen. This, also combined with the lack of hashed password, discloses any user on the system's password, username, and other information stored within the database.

Example:

When logged in as a non administrative user a user can go to `edit_user.php?user_id=1` and view the default admin account's password. Changing the `user_id` variable discloses the corresponding account's data.

Workaround:

Enabling Magic Quotes will negate the XSS and SQL injection attacks on affected systems.

ADDITIONAL INFORMATION

The information has been provided by [<mailto:security@xxxxxxxxxxxxxxxxxx>](mailto:security@xxxxxxxxxxxxxxxxxx) Mayhemic Labs.

The original article can be found at:

[<http://www.mayhemiclabs.com/advisories/MHL-2006-002.txt>](http://www.mayhemiclabs.com/advisories/MHL-2006-002.txt)
<http://www.mayhemiclabs.com/advisories/MHL-2006-002.txt>

=====

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@xxxxxxxxxxxxxxxx`

In order to subscribe to the mailing list, simply forward this email to: `list-subscribe@xxxxxxxxxxxxxxxx`

=====

=====

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.