

[UNIX] Credit Card Data Disclosure in CitrusDB

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0038.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/13/05

To: list@securiteam.com

Date: 13 Feb 2005 12:34:51 +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>

Credit Card Data Disclosure in CitrusDB

SUMMARY

<<http://www.citrusdb.org/>> CitrusDB is "an open source customer database application that uses PHP and a database backend (currently MySQL) to keep track of customer information, services, products, billing, and customer service information".

CitrusDB uses a textfile to temporarily store credit card information.

This textfile is located in the web tree via a static URL and thus accessible to third parties. It also isn't deleted after processing resulting in a big window of opportunity for an attacker..

DETAILS

Vulnerable Systems:

- * CitrusDB version 0.3.5 and prior

Immune Systems:

- * CitrusDB version 0.3.6 or newer

The URL to the textfile "<path to CitrusDB>/io/newfile.txt" is stated in the files "tools/uploadcc.php" and "tools/importcc.php". The <path to CitrusDB> is always known while surfing. Therefor also "newfile.txt"

Securiteam: [UNIX] Credit Card Data Disclosure in CitrusDB

containing the credit card data can be easily found and accessed. This leads to disclosure of the confidential data stored in that file.

Workaround:

Either deny access to the file using access restriction features of your webserver or change CitrusDB to use a file outside document root and not accessible via HTTP.

Fix:

Update to CitrusDB version 0.3.6 or higher and set the \$path_to_ccfile in the configuration to a path not accessible via HTTP.

ADDITIONAL INFORMATION

The information has been provided by
<mailto:dornseif@informatik.rwth-aachen.de> Maximillian Dornseif.
The original article can be found at:
<<http://tsyklon.informatik.rwth-aachen.de/redteam/rt-sa-2005-001>>
<http://tsyklon.informatik.rwth-aachen.de/redteam/rt-sa-2005-001>

=====

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.