

Securiteam: [UNIX] Buffer Overflow in PostgreSQL (cash_words)

[UNIX] Buffer Overflow in PostgreSQL (cash_words)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0085.html>

From: support@securiteam.com

Date: 08/21/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 21 Aug 2002 19:06:44 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Buffer Overflow in PostgreSQL (cash_words)

SUMMARY

PostgreSQL is an advanced object-relational database management system that supports an extended subset of the SQL standard, including transactions, foreign keys, subqueries, triggers, user-defined types, and functions.

There exists a stack based buffer overflow in `cash_words()` function, that potentially allows an attacker to execute malicious code.

DETAILS

How to reproduce:

```
psql> select cash_words('-70000000000000000000000000000000');
```

```
pgReadData() --- backend closed the channel unexpectedly.
```

```
... ..
```

The connection to the server was lost...

Solution:

Upgrade to version 7.2.1.

Securiteam: [UNIX] Buffer Overflow in PostgreSQL (cash_words)

ADDITIONAL INFORMATION

The information has been provided by <mailto:mordred@s-mail.com> Sir Mordred The Traitor.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NEWS] More Vulnerabilities with Pingtel Xpressa SIP-based IP Phones"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)