

[NT] Microsoft SQL Server 2000 pwdencrypt() Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0052.html>

From: support@securiteam.com

Date: 06/15/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 15 Jun 2002 21:23:20 +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.

Microsoft SQL Server 2000 pwdencrypt() Buffer Overflow

SUMMARY

Microsoft SQL Server 2000's pwdencrypt() stored procedure has been found to contain an exploitable buffer overflow, the overflow is caused by providing large buffer to the function.

DETAILS

Vulnerable systems:

* Microsoft SQL Server 2000 (up to SP2)

Microsoft SQL Server's contains two undocumented password encryption functions, pwdencrypt and pwdcompare, one of these functions, pwdencrypt has been found to contain a remotely exploitable buffer overflow.

Example:

```
SELECT pwdencrypt(REPLICATE('A',353))
```

Vendor status:

The vulnerability was confirmed by Microsoft but has not yet provided information on when a patch will be released.

Securiteam: [NT] Microsoft SQL Server 2000 pwdencrypt() Buffer Overflow

ADDITIONAL INFORMATION

Information on the two undocumented functions can be found at:

<<http://www.sqlmag.com/Articles/Index.cfm?ArticleID=9809>>

<http://www.sqlmag.com/Articles/Index.cfm?ArticleID=9809>

The information has been provided by <<mailto:jimmers@yandex.ru>> martin rakhmanoff.

=====

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: "[NT] Buffer Overflow in Microsoft Rasapi32.dll"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)