

[TOOL] dSQLSRVD, SQL Server SysComments Decryptor

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-12/0101.html>

From: support@securiteam.com

Date: 12/23/01

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 23 Dec 2001 05:14:45 +0100 (CET)

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.

dSQLSRVD, SQL Server SysComments Decryptor

DETAILS

<<http://www.geocities.com/d0mn4r/dSQLSRVD.html>> dSQLSRVD – dOMNAR's SQL Server SysComments Decryptor – has been designed to assist developers and administrators of SQL Server 7 and 2000 with examining stored procedures, triggers, views and user-defined functions, in order to gain better insight into 3rd party applications and their database functionality. Such a task is often necessary when integrating a new system with a company's existing systems, or when optimizing a database server's performance.

Unfortunately, some companies insist on using the "With Encryption" clause in their T-SQL-code, which prevents the use of sp_helptext, the stored procedure normally used to extract the stored T-SQL-definition from the syscomments system-table. Why they do this is a puzzle, since encrypting something that can be decrypted without user interaction (i.e., entering of a password) isn't anything else than the infamous security by obscurity. Such "security" can always be broken in short time (speaking in cryptological terms), and offers no real security, which this utility is a proof of. It should be pointed out that Microsoft does not use the encryption clause for any of its own code accompanying SQL Server.

Securiteam: [TOOL] dSQLSRVD, SQL Server SysComments Decryptor

SQL Server encryption notes:

For SQL Server 7 you will only need an account with read-access on the syscomments table, which is the default. The encryption algorithm uses a static key for all encrypted entries.

In SQL Server 2000, Microsoft improved the encryption somewhat, so that it is now impossible for accounts that are not members of the SysAdmin role to decrypt syscomments entries. This is because they changed the encryption algorithm to use dynamically calculated keys based on certain database specific information that can only be read by SysAdmins. Because of the algorithms used, brute forcing would not be a feasible solution.

ADDITIONAL INFORMATION

The tool can be downloaded from:

<<http://www.geocities.com/d0mn4r/dSQLSRVD.html>>
<http://www.geocities.com/d0mn4r/dSQLSRVD.html>

The information has been provided by dOMNAR.

=====

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: "[UNIX] Glibc Globing Issues (~AAA{ Trick})"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)