

[NT] XDICT Buffer Overrun Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0024.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/07/04

To: list@securiteam.com

Date: 7 Nov 2004 18:05:57 +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>

XDICT Buffer Overrun Vulnerability

SUMMARY

<<http://www.kingsoft.com>> XDICT is a very popular translation Software (CHINESE ENGLISH) in China.

While using the XDICT's 'Screen Fetch' feature it is possible to overflow a buffer within XDICT and cause arbitrary code execution.

DETAILS

Vulnerable Systems:

- * XDICT 2002
- * XDICT 2003
- * XDICT 2004
- * XDICT 2005

When using the 'Screen Fetch' feature of XDICT that allows for fetching of the word from the screen, XDICT automatically traces mouse input and returns the translation of the word or sentence pointed.

When pointing on a word, XDICT will copy the text to an internal buffer and will begin searching for the translation in it's dictionary. A long word or sentence can be used to overflow the internal buffer used and will

Securiteam: [NT] XDICT Buffer Overrun Vulnerability

cause the process to consume all CPU resources which will hang and then crash the erroneous process. It is interesting to note that XDICT 2005 on Win2K Pro+ will gracefully quit instead of crashing.

In order to demonstrate this bug, open notepad and type in at least 88 characters (i.e.: 'A' x 88) with no spaces in between. Using the mouse and pointing on the word, the contents will be copied and the buffer overflowed, enabling an attacker the ability to execute code on the target machine with proper malicious input.

Vendor Status:

2004.10.26 Vendor notice

2004.10.27 The vendor reply that this bug is submitted to the TEST department NO further reply

ADDITIONAL INFORMATION

The information has been provided by <mailto:smaillist@gmail.com> Sowhat

The original article can be found at:

<<http://secway.org/Advisory/Ad20041026EN.txt>>

<http://secway.org/Advisory/Ad20041026EN.txt>

=====

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.