

# [VulnWatch] [GOODFELLAS – VULN] BarCodeAx.dll v. 4.9 ActiveX Control Remote Stack Buffer Overflow

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-06/msg00003.html>

---

- *From:* GOODFELLAS SRT <[goodfellas@xxxxxxxxxxxxxxxxxxx](mailto:goodfellas@xxxxxxxxxxxxxxxxxxx)>
  - *Date:* Sat, 23 Jun 2007 13:03:15 -0300
- 

.: GOODFELLAS Security Research TEAM .:  
.: <http://goodfellas.shellcode.com.ar> .:

BarCodeAx.dll v. 4.9 ActiveX Control Remote Stack Buffer Overflow

=====  
Internal ID: VULWAR200706223

## Introduction

-----

BarCodeAx.dll is a library included in the Barcode ActiveX software package from the Company RKD:  
(<http://www.barcodetools.com/barcode/barcode-activex/barcode-activex.html>)

Such package allows to manage the printing of different barcodes.

One of the BarCodeAx.dll exported methods is vulnerable to a stack buffer overflow which can be remotely exploited.

## tested in

-----

- Windows XP SP2 english/french with IE 6.0 / 7.0
- windows vista Professional SP1 with IE 7.0

## Summary

-----

The BeginPrint method fail to correctly check the size of the arguments that receives, causing a stack buffer overflow.

## Impact

-----

Any application that uses the said ActiveX to control barcodes would be exposed to remote code execution.

### Workaround

- 
- Activate the Kill bit zero in  
CLSID:C26D9CA8–6747–11D5–AD4B–C01857C10000
- Unregister BarCodeAx.dll using regsvr32

### Timeline

- 
- June 21, 2007 -- Bug discovery
- June 22, 2007 -- Bug published

### Credits

- 
- \* Brian Mariani <bmariani@xxxxxxxxxxxxxxxxxxxx>
- \* GoodFellas Security Research Team <goodfellas.shellcode.com.ar>

### Technical Detail

-----

Vulnerable method.

```
Sub BeginPrint (  
ByVal name As String  
)
```

We need 656 bytes to overflow the buffer and rewrite EBP + EIP.

```
– Reversing  
7C97DF40 PUSH 0  
7C97DF42 PUSH ESI  
7C97DF43 CALL 7C97CDC9  
7C97DF48 MOV EBX,[EBP+10]  
7C97DF4B LEA EDI,[EBX-8]  
7C97DF4E MOV [EBP-2C],EDI  
7C97DF51 MOVZX EAX,WORD PTR [EDI] <---- CRASH  
7C97DF54 SHL EAX,3  
7C97DF57 MOV [EBP-30],EAX  
7C97DF5A PUSH 7C97E11C  
7C97DF5F PUSH EDI  
7C97DF60 PUSH ESI  
7C97DF61 CALL 7C97CC6D  
7C97DF66 TEST AL,AL  
7C97DF68 JE 7C97E0BF
```

– Registers

[VulnWatch] [GOODFELLAS – VULN] BarCodeAx.dll v. 4.9 ActiveX Control Remote Stack Buffer Overflow

EIP 41414141  
EAX C0040204  
EBX 00407830 -> 003E977D  
ECX 0013ECE8 -> Asc:  
AA  
EDX 00150608 -> 7C98C500  
EDI 00000000  
ESI 001844CC -> 00180008  
EBP 41414141  
ESP 0013EBE8 -> Asc:  
AA

--  
GOODFELLAS (Shellcode Security Research)  
<http://goodfellas.shellcode.com.ar>

**Attachment: signature.asc**  
*Description:* This is a digitally signed message part

[VulnWatch] [GOODFELLAS – VULN] BarCodeAx.dll v. 4.9 ActiveX Control Remote Stack Buffer Overflow