

[NEWS] Adobe Reader Subroutine Pointer Overwrite

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-01/msg00028.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 10 Jan 2007 15:04:58 +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>

Adobe Reader Subroutine Pointer Overwrite

SUMMARY

<<http://www.adobe.com/products/acrobat/>> Adobe Reader is "the most popular program for viewing documents in Adobe Portable Document Format (PDF)". A vulnerability in Adobe Reader allows a specially crafted PDF file to trigger a pointer overwrite, which in turn can be used to execute arbitrary code.

DETAILS

Vulnerable Systems:

- * Adobe Reader version 7.0.8 and prior

Immune Systems:

- * Adobe Reader 7.0.9

The problem exists when the Adobe product is trying to render a specially crafted PDF file.

Take a look at this code snippet:

-----// SNIP SNIP //-----

[NEWS] Adobe Reader Subroutine Pointer Overwrite

```
0:000> u 08009d3f
CoolType+0x9d3f:
08009d3f 83e904 sub ecx,0x4
08009d42 890da07a1d08 mov [CoolType!CTCleanup+0xb393b
081d7aa0)],ecx
08009d48 ffb49070fefff push dword ptr [eax+edx*4-0x190]
08009d4f 8b09 mov ecx,[ecx]
08009d51 51 push ecx
08009d52 ff506c call dword ptr [eax+0x6c] ; (*)
08009d55 59 pop ecx
08009d56 59 pop ecx
-----// SNIP SNIP //-----
```

Instruction at 0x08009d52 call the location which address is stored at [eax+0x6c]. Value of the eax points somewhere inside the allocated heap memory block, as shown here:

```
-----// SNIP SNIP //-----
..
K: 199 -> [*] HeapAlloc(0x3E0000,0x0,0x4(4))=0x16F6FF8 end at: 0x16F6FFC
K: 200 -> [*] HeapAlloc(0x3E0000,0x0,0x4F4(1268))=0x16F6958 end at:
0x16F6E4C
K: 201 -> [*] HeapAlloc(0x3E0000,0x0,0xFE30(65072))=0x16F6E58 end at:
0x1706C88
K: 202 -> [*] HeapAlloc(0x3E0000,0x0,0x304(772))=0x1706C90 end at:
0x1706F94
K: 203 -> [*] HeapAlloc(0x3E0000,0x0,0xFE24(65060))=0x1706FA0 end at:
0x1716DC4 <- THIS ONE
-----// SNIP SNIP //-----
```

[EAX+0x6c] points to 0x222C offset from beginning of the last heap memory block.

When specially badly created PDF file is being render, there exist a possibility to cause a memory corruption, which leads to the overwrite of the subroutine address stored at [eax+0x6c].

Here's the debugger snippet, after calling overwritten [eax+0x6c] (note the heap base block is different then previously mentioned, its just another independent session):

```
-----// SNIP SNIP //-----
(25a0.2170): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=016f4320 ebx=00000000 ecx=baadf00d edx=00000069 esi=016f4ab9
edi=016f14b4 eip=baadf00d esp=0012deec ebp=0012df80 iopl=0 nv up ei pl nz
na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=0038 gs=0000 efl=00010202
*** ERROR: Symbol file could not be found. Defaulted to export symbols
for C:\Program Files\Adobe\Acrobat 7.0\Reader\CoolType.dll -
```

[NEWS] Adobe Reader Subroutine Pointer Overwrite

baadf00d ?? ???

-----// SNIP SNIP //-----

The attacker can control EIP register, this may lead to a potencial code execution in context of current user.

Impact:

Successful exploitation may allow the attacker to run arbitrary code in context of user running Adobe Reader.

Vendor response:

All pathes are available, via auto-update or

<<http://www.adobe.com/go/getreader/>> <http://www.adobe.com/go/getreader/>.

Disclosure Timeline:

03/09/2006 – Advisory sent to ADOBE PSIRT

03/09/2006 – Initial Vendor Response

11/09/2006 – Vendor confirms the vulnerability.

09/01/2007 – Security Bulletin ready, advisory released.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5857>>

CVE-2006-5857

ADDITIONAL INFORMATION

The information has been provided by <<mailto:bania.piotr@xxxxxxxxxx>> Piotr Bania.

The original article can be found at:

<<http://www.piotrbania.com/all/adv/adobe-acrobat-adv.txt>>

<http://www.piotrbania.com/all/adv/adobe-acrobat-adv.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@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, loss of business profits or special damages.