Authorisation.
Jason Edelstein

Release date.
06 October 2010.

Sense of Security – Security Advisory – SOS-10-003.

Adobe Reader 9.3.4 Multiple Memory Corruption Vulnerabilities.

06 October 2010.

Adobe Reader Multiple Memory Corruption - Security Advisory - SOS-10-003

Release Date.	06-Oct-2010
Last Update.	-
Vendor Notification Date.	26-Jul-2010
Product.	Adobe Reader Adobe Acrobat
Platform.	Microsoft Windows
Affected versions.	9.3.4 verified and possibly others
Severity Rating.	Medium
Impact.	Denial of service, potentially code execution.
Attack Vector.	Local system
Solution Status.	Vendor patch
CVE reference.	CVE-2010-3630

Details.

Adobe Reader is a popular freeware PDF viewer. Version 9.3.4 of the application is vulnerable to multiple memory corruption vulnerabilities. By sending specially crafted PDF files it is possible to cause memory corruption in the 3difr and AcroRd32.dll modules. Both issues trigger a null pointer condition which result in an access violation. The issue in AcroRd32.dll is triggered when Adobe Reader is closed.

Function sub_60AF56 in AcroRd32.dll access violates when attempting to read data pointed to by the ESI register. Part disassembly of the function is shown below:

```
push    ebp
mov     ebp, esp
sub     esp, 1Ch
and     [ebp+var_4], 0
push    ebx
push    esi
mov     esi, ecx
mov     ebx, [esi+23Ch] <-- crash
```

Function sub_1000EEE0 in 3difr also access violates when attempting to read data pointed to by the ESI register the ECX register. Part disassembly of the function is shown below:

```
mov     ecx, [eax+4]
mov     eax, [edx+4]
mov     dx, [eax]
cmp     dx, [ecx] <-- crash
jnz    short loc_1000EF87
```

It may be possible to exploit these vulnerabilities to execute arbitrary code under the context of the user running Adobe Reader.

Proof of concept.

Proof of concept PDF files are available to Sense of Security customers upon request.

Solution.

A patch is available from Adobe and is included in the next release (9.4).

Discovered by.

Brett Gervasoni from Sense of Security Labs.

About us.

Sense of Security is a leading provider of information security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia's premier application penetration testing firm and trusted IT security advisor to many of the countries largest organisations.

Sense of Security Pty Ltd

Level 8, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au

E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-10-003.pdf

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php