



## Securing your web world

### Buffer Overflow Issue In Certain Versions of Adobe Acrobat and Acrobat Reader May Cause Remote Code Execution 02/22/2009

#### Vulnerability Details

A vulnerability has been found in version 9.0.0 and earlier of the Adobe Acrobat family of applications that may cause the program(s) to crash, as well as allow a remote user to execute malicious code on an affected system.

It exploits a vulnerability in a non-JavaScript function call; however JavaScript is also used to successfully execute malicious code. Disabling JavaScript will prevent code execution, but not crashes of Adobe Acrobat.

#### Affected Software

- Adobe Acrobat Pro 9.0.0 and earlier versions
- Adobe Acrobat Pro Extended 9.0.0 and earlier versions
- Adobe Acrobat Reader 9.0.0 and earlier versions
- Adobe Acrobat Standard 9.0.0 and earlier versions

As of this time, no patch exists for this vulnerability. A patch for Acrobat and Acrobat Reader versions 9.0.0 is expected by March 11, 2009. Patches for earlier versions will follow.

Please consult the official [Adobe security bulletin](#) for details on these patches.

#### Workaround

Third-party applications capable of opening PDF documents are not affected by this vulnerability. Users may use these applications to read and produce PDF files.

Steps to work around this vulnerability may be found at the [US-CERT](#) Technical Cyber Security Alert TA09-051A.

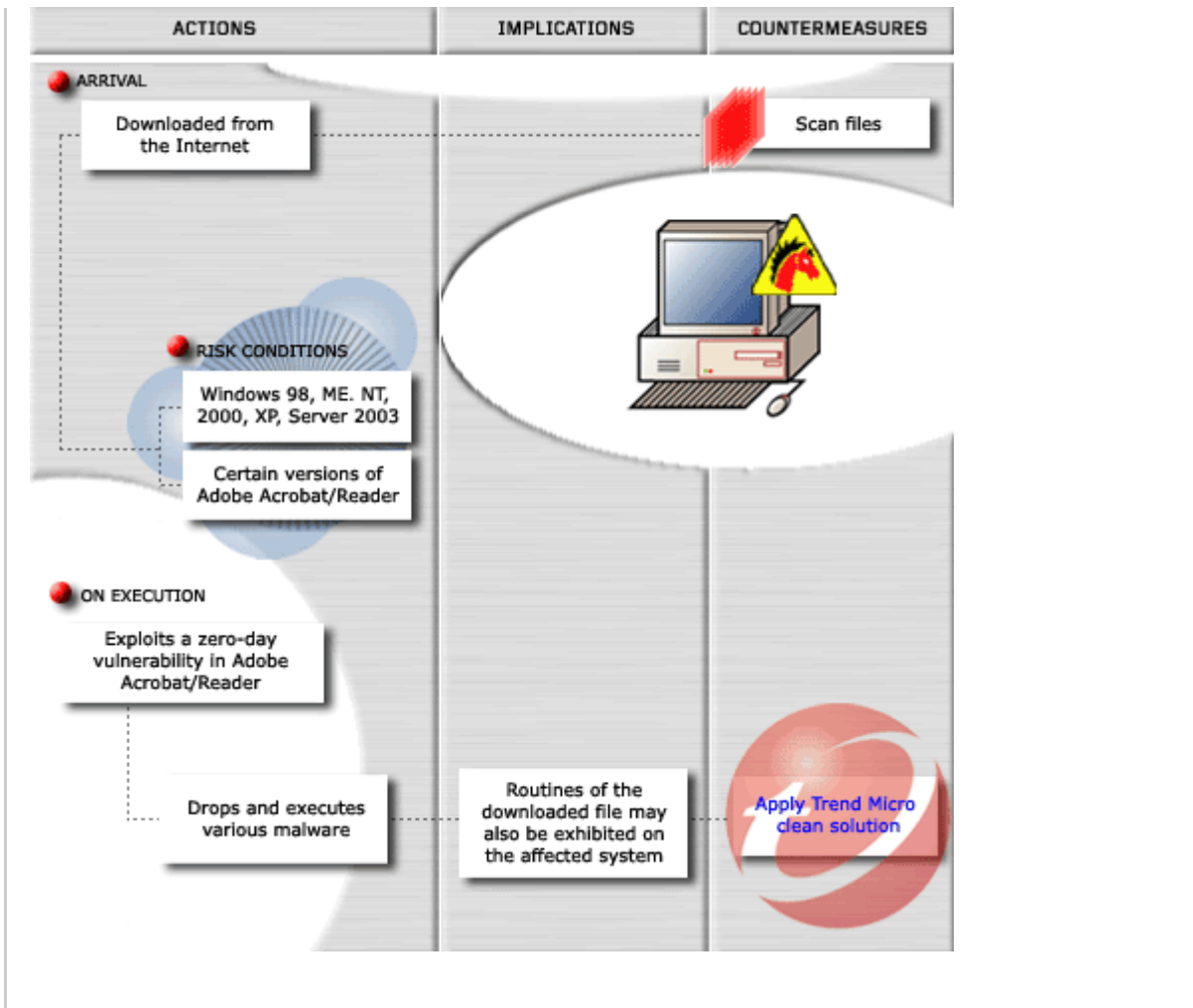
#### Malware exploits a zero-day vulnerability

This Trojan is a specially crafted .PDF file that exploits a zero-day vulnerability in Acrobat Reader Version 8.x and 9.0.

The said vulnerability causes the application to crash and could potentially allow an attacker to take control of the affected system.

Differing variants of this file drop various malware onto the affected system. Below are some of the malware detected by Trend Micro that are dropped malwares by this PDF:

BKDR\_NETCL.A  
EXPL\_EXECOD.A  
JS\_SHELLCOD.JS  
TROJ\_AGENT.ZWQA  
TROJ\_FAKEAV.LKQQ



**Recommended Action**

- Keep your Trend Micro products up-to-date with the current pattern files (All detections are currently available in our Official Pattern)
- Use caution when opening email attachments or when using peer-to-peer file sharing, instant messaging, or chat rooms

**Additional Information**

<http://blog.trendmicro.com/portable-document-format-or-portable-malware-format/>  
<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FPIDIEF%2EIN&VSect=T>