

# [NT] Adobe Download Manager AOM Stack Buffer Overflow

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00007.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 6 Dec 2006 16:34:50 +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 Download Manager AOM Stack Buffer Overflow

---

## SUMMARY

eEye Digital Security has discovered a stack buffer overflow in Adobe Download Manager, a utility typically installed for the purpose of downloading Adobe software such as Adobe (Acrobat) Reader. By opening a malicious AOM file, a user's system may be compromised by arbitrary code within the file, which executes with the privileges of that user.

## DETAILS

Vulnerable Systems:

- \* Adobe Download Manager versions 2.1.x and earlier

A web-based attack conducted through Internet Explorer may succeed without the use of ActiveX or scripting, and without any additional user interaction other than viewing a web page, if the web server indicates a Content-Type of "application/aom" when serving up the malicious AOM file. In such a case, an ".aom" file extension is not required.

AdobeDownloadManager.exe is responsible for extracting download instructions from AOM files, which are essentially XML with an appended

## [NT] Adobe Download Manager AOM Stack Buffer Overflow

CRC32 in decimal, and committing the instructions to the file "%APPDATA%\dm.ini" for later processing. For instance, opening the following AOM file:

```
<?aom encoding="UTF-8"?>
<AdobeDownloadManager>
</AOM>
<DownloadRecord>
<url>WelcomeToMyHumbleAdobe</url>
</DownloadRecord>
</AOM>
</AdobeDownloadManager>3871966612
```

Will generate the following lines in "dm.ini":

```
[STARTUP]
Status=IncompleteDownload
[WelcomeToMyHumbleAdobe]
StoreID=0
TransactionID=0
```

When launched, whether or not it is supplied with an AOM file, AdobeDownloadManager.exe reads the entries from "dm.ini" and handles each described download according to its properties. It begins by reading a list of section names into a 400h-byte buffer using GetPrivateProfileStringA, then copies each section name into a 108h-byte stack buffer using strncpy with a length limit equal to the length of the section name string. The result is a relatively straightforward stack buffer overflow, with the only complication being the character restrictions.

It should be possible to uninstall Adobe Download Manager, or at least unassociate the AOM file extension and "application/aom" Content-Type in the registry, to defend against this vulnerability. Hopefully users who have been forced to install Adobe Download Manager realized its superfluousness and have already uninstalled it.

Vendor Status:

Adobe has released a patch for this vulnerability which is available at:

<<http://www.adobe.com/products/acrobat/acrrmanager.html>>  
<http://www.adobe.com/products/acrobat/acrrmanager.html>.

The vendor bulletin is available at:

<<http://www.adobe.com/support/security/bulletins/apsb06-19.html>>  
<http://www.adobe.com/support/security/bulletins/apsb06-19.html>.

### ADDITIONAL INFORMATION

The information has been provided by eEye.

The original article can be found at:

<<http://research.eeye.com/html/advisories/published/AD20061205.html>>

[NT] Adobe Download Manager AOM Stack Buffer Overflow

<http://research.eeye.com/html/advisories/published/AD20061205.html>

=====

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.