

[UNIX] Multiple Apple Mac OS X AppleTalk

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-11/msg00034.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 19 Nov 2007 17:26:12 +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>

Multiple Apple Mac OS X AppleTalk

SUMMARY

AppleTalk, "a set of networking protocols developed by Apple, was originally implemented on early Mac operating systems. Although it is a legacy protocol, it is still supported on the latest version of Mac OS X. AppleTalk is compiled into the default kernel, but must be turned on in order to be used".

<<http://docs.info.apple.com/article.html?artnum=50039>> ASP, as its name implies, is "a Session Layer protocol that is used by the AppleTalk File Sharing protocol to establish connections with a peer".

Multiple vulnerabilities have been discovered in Apple Mac OS X's AppleTalk.

DETAILS

Vulnerable Systems:

- * Mac OS X version 10.4.10

Apple Mac OS X AppleTalk ASP Message Kernel Heap Overflow Vulnerability
Local exploitation of a heap based buffer overflow in Apple Inc.'s OS X

[UNIX] Multiple Apple Mac OS X AppleTalk

may allow an attacker to execute arbitrary code in kernel context.

The vulnerability exists within a function responsible for sending an ASP (AppleTalk Session Protocol) message on an AppleTalk socket. When allocating a buffer, the kernel uses a user provided integer to perform an arithmetic operation that calculates the number of bytes to allocate. This calculation can overflow, leading to the allocation of a buffer of insufficient size. This results in an exploitable heap based buffer overflow within the kernel.

Analysis:

Successful exploitation of this vulnerability will result in the execution of arbitrary code in kernel context. Exploitation has proven to be non-trivial.

In order to reach the vulnerable code, a system would have to have AppleTalk turned on. It would likely be used on a network consisting of older Mac hosts since previous versions of Mac relied on it to implement Apple File Sharing.

Workaround:

Disabling AppleTalk will prevent exploitation of this vulnerability. Executing the following command will disable AppleTalk if it is enabled.

```
# appletalk -d
```

Vendor response:

Apple addressed this vulnerability within their Mac OS X 2007-008 security update. More information is available at the following URL.

<http://docs.info.apple.com/article.html?artnum=307041>

<http://docs.info.apple.com/article.html?artnum=307041>

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4269>

CVE-2007-4269

Disclosure Timeline:

08/08/2007 – Initial vendor notification

08/09/2007 – Initial vendor response

11/14/2007 – Public disclosure

Apple Mac OS X AppleTalk Socket IOCTL Kernel Stack Buffer Overflow Vulnerability

Local exploitation of a stack based buffer overflow in Apple Inc.'s OS X may allow an attacker to execute arbitrary code in kernel context.

The vulnerability exists within the function responsible for adding an AppleTalk zone to an interface's routing table. A zone can be thought of as something similar to a Windows Domain.

When copying the user provided zone information into a fixed size stack

[UNIX] Multiple Apple Mac OS X AppleTalk

buffer, the kernel uses a user provided length as the number of bytes to copy into the destination buffer. This results in an exploitable stack buffer overflow in the kernel.

Analysis:

Successful exploitation of this vulnerability will result in the execution of arbitrary code in kernel context. Unsuccessful attempts will likely crash the system.

In order to exploit this vulnerability, the system needs to have AppleTalk configured in routing mode. This is not enabled by default. It would likely be enabled on a Mac system running on a network with legacy Mac hosts.

Workaround:

Disabling AppleTalk will prevent exploitation of this vulnerability. Executing the following command will disable AppleTalk if it is enabled.

```
# appletalk -d
```

Vendor response:

Apple addressed this vulnerability within their Mac OS X 2007-008 security update. More information is available at the following URL.

<<http://docs.info.apple.com/article.html?artnum=307041>>

<http://docs.info.apple.com/article.html?artnum=307041>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4267>>

CVE-2007-4267

Disclosure Timeline:

08/08/2007 – Initial vendor notification

08/09/2007 – Initial vendor response

11/14/2007 – Public disclosure

Apple Mac OS X AppleTalk mbuf Kernel Heap Overflow Vulnerability
Local exploitation of a heap based buffer overflow in Apple Inc.'s OS X may allow an attacker to execute arbitrary code in kernel context.

The vulnerability exists within a function responsible for allocating an mbuf. mbufs are a BSD concept, long used by BSD kernels to allocate buffers for storing network related data.

When allocating an mbuf buffer, the kernel performs a comparison using two signed integers, one of which is controlled by the user, to determine how many bytes to allocate. If a user passes a negative value, a minimally sized buffer will be allocated due to the signed comparison. The calling function will usually interpret the user controlled value as an unsigned value, and this results in the allocated buffer being overflowed.

Analysis:

[UNIX] Multiple Apple Mac OS X AppleTalk

Successful exploitation of this vulnerability will result in the execution of arbitrary code in kernel context. Unsuccessful attempts will likely crash the system. Exploitation has proven to be non-trivial.

In order to exploit this vulnerability, a system would have to have AppleTalk turned on. It would likely be used on a network consisting of older Mac hosts since previous versions of Mac relied on it to implement Apple File Sharing.

Workaround:

Disabling AppleTalk will prevent exploitation of this vulnerability. Executing the following command will disable AppleTalk if it is enabled.

```
# appletalk -d
```

Vendor response:

Apple addressed this vulnerability within their Mac OS X 2007-008 security update. More information is available at the following URL.

<<http://docs.info.apple.com/article.html?artnum=307041>>

<http://docs.info.apple.com/article.html?artnum=307041>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4268>>

CVE-2007-4268

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idefense-labs-advisories@xxxxxxxxxxxxx>> iDefense Labs Security Advisories.

To keep updated with the tool visit the project's homepage at:

<<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=629>>

<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=629>,

<<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=628>>

<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=628>

and

<<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=627>>

<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=627>

=====

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@xxxxxxxxxxxxx

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

=====

=====

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.