

[NEWS] Mac OS X HFS+ Multiple Vulnerabilities (__Fork)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0077.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 02/21/05

To: list@securiteam.com

Date: 21 Feb 2005 12:54:19 +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>

Mac OS X HFS+ Multiple Vulnerabilities (__Fork)

SUMMARY

Hierarchical File System Plus(HFS+) is "a file system developed by Apple Computer for use on computers running Mac OS".

HFS+ allow servers such as Apache to retrieve the source of a PHP or JSP source files using the data and resource fork options.

DETAILS

Vulnerable Systems:

- * MacOS X version 10.2 and above

Apple's HFS and HFS+ file systems allows two separate data streams for each file, referred to as the "data fork" and "resource fork". The classic Mac OS operating systems and Carbon API on Mac OS X provide separate functions for opening and manipulating the data and resource forks. In Mac OS X, however, support for addressing these separate streams has been integrated into the POSIX API. In Mac OS X 10.2 and above, opening the file by its pathname opens the data fork, but the data fork or resource fork may also be opened for a given file by respectively appending

Securiteam: [NEWS] Mac OS X HFS+ Multiple Vulnerabilities (__Fork)

"/.namedfork/data" or "/.namedfork/rsrc" to the pathname passed to the open(2) system call. In previous versions, they may be addressed by appending the special pathnames "/.__Fork/data" or "/.__Fork/rsrc". The resource fork may also be opened in most versions of Mac OS X by appending "/rsrc" to the file pathname.

Due to this feature being available throughout the operating system, via the POSIX API, it is therefore available to any software involved in the opening of file streams via the open() syscall, such as a web server opening an HTML or PHP file present on the Darwin servers file system. As a result, server daemons, such as web servers which open file streams, based on user controlled data, may be fooled into opening the respective files resource and/or file fork rather than the absolute file name. This may allow users to view arbitrary data, such as the source code of server interpreted documents (such as PHP and JSP files).

Workaround:

The HFS+ file system is not recommended for dedicated servers, but is required to support numerous legacy Macintosh applications. At the time of this technical advisory, it is strongly recommended that organizations with public Internet-facing Apple servers consider migration to the Berkeley Fast File System (FFS/UFS) option available in OS X.

ADDITIONAL INFORMATION

The information has been provided by <mailto:tac@netsec.net> TAC.

=====

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@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

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.