

[NEWS] Mac OS X malloc() Local Privilege Escalation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0112.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/29/05

To: list@securiteam.com

Date: 29 Sep 2005 11:06:14 +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 malloc() Local Privilege Escalation

SUMMARY

The Mac OS X malloc() function uses environment variables that can be modified by a local attacker and used to perform a privilege escalation attack.

DETAILS

Vulnerable Systems:

- * Mac OS X prior to Apple security update 2005-008

The malloc() function within the libSystem library on Mac OS X uses several environment variables to enable various logging functionality. The description of one of these variables, "MallogLogFile" taken from the manual page is shown below:

```
MallogLogFile <f> Create/append messages to the given
file
                path <f> instead of writing to the
standard
                error.
```

Securiteam: [NEWS] Mac OS X malloc() Local Privilege Escalation

An error exists in the fact that malloc() will still pay attention to this variable when an application is suid root.

The following code taken from libSystem (libc) illustrates this:

```
flag = getenv("MallocLogFile");
if (flag) {
    if (flag) {
        fd = open(flag, O_WRONLY|O_APPEND|O_CREAT, 0644);
        if (fd >= 0) {
            malloc_debug_file = fd;
            fcntl(fd, F_SETFD, 0); // clear close-on-exec flag XXX
why?
        } else {
            malloc_printf("Could not open %s, using stderr\n",
flag);
        }
    }
}
```

A malicious user can set this variable before running a suid application in order to modify any file on the system. This can be used in order to trivially escalate privileges on the system.

Vendor Status:

The vendor has issued a fix to the issue in Security Update 2005-008.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2748>>
CAN-2005-2748

ADDITIONAL INFORMATION

The information has been provided by <<mailto:advisories@suresec.org>>
Suresec Advisories.

The original article can be found at:

<<http://www.suresec.org/advisories/adv7.pdf>>
<http://www.suresec.org/advisories/adv7.pdf>

=====

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.