suresec
SECURING THE SOURCE

Suresec security advisory 7
September 25, 2005
CVE-ID: CAN-2005-2748

malloc() logging enabled for suid applications.

Vulnerability summary:
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:

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

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) {
        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);
        }
    }
```

Impact:
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.

Affected versions:
This vulnerability affects all versions of Mac OS X below Apple security update 2005-008.

Suggested Recommendations:
Applying Security Update 2005-008 will address this vulnerability.

Credits:

This vulnerability was found by Ilja van Sprundel.

About us:
Suresec Ltd is a global service provider of Internet security solutions and consultancy with unmatched quality from our world class consultancy practice.
Our consultants have pioneered in the field of security research and have closely worked with leading software companies and service providers to mitigate risks and fix a number of critical vulnerabilities, Suresec also works closely with a number of open source companies
to provide them with a source code auditing and technical consultancy.
We have a strong team consultants spread across Europe, the United States of America And Australia specializing in security consulting.