



sureSEC
SECURING THE SOURCE

Suresec security advisory 3
Release date: 9 June 2005

Mac OS X 10.4 launchd Local root Vulnerability

About launchd (taken from the launchd man-page):

"**launchd** manages daemons, both for the system as a whole and for individual users. Ideal daemons can launch on demand based on criteria specified in their respective XML property lists located in one of the directories specified in the FILES section.

During boot **launchd** is invoked by the kernel to run as the first process on the system and to further bootstrap the rest of the system."

Vulnerability summary:

The launchd tool, when invoked, uses the `launchd_server_init()` function to set up temporary files in the `/tmp` directory. It first creates a directory with the name of the invoking user's current uid. It then uses the `chown()` function to modify the ownership of the directory to belong to the invoking user.

After this has occurred a socket (file) is created inside this directory and the `chown()` function is again called to give this file ownership permissions of the invoking user.

A race condition exists here. If a malicious user removes the newly created socket and replaces it with a symbolic link to **any** file which they don't own. If this is timed to be in between the function call to create the socket, and the `chown()` call the symbolic link will be followed. This gives the malicious user the ability to effectively "steal" the ownership of any file or directory on the system.

Impact:

Successful exploitation of this vulnerability will allow a malicious user to "steal" ownership of any file on the system. Using this to gain access to a root shell is a trivial process.

Affected Versions:

This vulnerability has been successfully exploited in `launchd 106`, which was shipped with Mac OS X 10.4 (Tiger).

Suggested Recommendations:

Efforts have been made to coordinate the release of this advisory with an update from Apple. Performing this update should eliminate the vulnerability.

Credits:

This vulnerability was found by Neil Archibald and 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 and Australia specializing in security consulting.