



sureSEC
SECURING THE SOURCE

Suresec security advisory 10
1th March 2006
CVE ID: CVE-2005-2713, CVE-2005-2714

Table of Contents

MacOSX /usr/bin/passwd file creation vulnerability	2
About passwd:.....	2
Vulnerability summary:	2
Impact:	3
Affected versions:	3
Suggested Recommendations:	3
Credits:	3
About us:	3

MacOSX /usr/bin/passwd file creation vulnerability

About passwd:

passwd is an extremely common unix utility used to change the password of user accounts on a system. The MacOSX passwd program can change passwords on different backend password storing systems, such as NetInfo, plain files, and LDAP.

Vulnerability summary:

The MacOSX passwd program supports multiple password storing systems, called infosystems. One of which is the unix based local flat-files.

When specifying this infosystem (via the -i parameter) it is possible to enter a path to a file. If this location file does not exist, it will get created by the password program.

Here in lies two vulnerabilities, one that allows a normal unprivileged user to create a file anywhere on the system, which will be owned by root.

The second vulnerability is that the umask is not setup by passwd, which means when the file is created, the unprivileged user can affect the file permissions on the newly created file.

umask is a mechanism to control what permissions are granted to files when being created. An example umask of 022 means that the group owner, and "other" users cannot write to the file. More information about umask can be found at ¹

The below code snippet shows the problem in greater depth:

```
int
file_passwd(char *uname, char *locn)
{
    char *ne, *oc, *nc;
    FILE *fp;
    char *fname;
    struct passwd *pw;
    struct passwd newpw;
    int uid;
```

1 <http://www.dartmouth.edu/~rc/help/faq/permissions.html>

```
    fname = _PASSWD_FILE;
    if (locn != NULL) fname = locn;

    fp = fopen(fname, "a+");
    ...
}
```

If the unprivileged user changes their umask to 0 (which means that no permissions are removed from the created file), the file pointed to by locn (which is specified by the user) will be created, with world writable privileges.

Impact:

When properly exploited this yields local root.

Affected versions:

This vulnerability affects MacOSX 10.3.x and 10.4.x up until 10.4.5, MacOSX 10.4.5 is no longer vulnerable to the umask bug, but still remains vulnerable to file creation bug.

Suggested Recommendations:

Update your MacOSX system, or as a workaround, removed the suid bit from the passwd program.

Credits:

Ilja van Sprundel found this vulnerability.

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.