

[VulnWatch] iDefense Security Advisory 03.02.06: Apple Mac OS X passwd Arbitrary Binary File Creation/Modification

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-03/msg00001.html>

- *From:* "labs-no-reply@xxxxxxxxxxxxx" <labs-no-reply@xxxxxxxxxxxxx>
 - *Date:* Thu, 02 Mar 2006 18:20:52 -0500
-

Apple Mac OS X passwd Arbitrary Binary File Creation/Modification

iDefense Security Advisory 03.02.06

<http://www.idefense.com/application/poi/display?type=vulnerabilities>

March 02, 2006

I. BACKGROUND

Mac OS X is an operating system for the Apple family of microcomputers. More information is available at the following link:

<http://www.apple.com/macosx/>

II. DESCRIPTION

Local exploitation of a design error in version 10.3.9 of Apple Computer Inc.'s Mac OS X could allow arbitrary files to be overwritten with user supplied contents.

The `/usr/bin/passwd` binary is a setuid application which allows users to change their password. There are two related vulnerabilities.

The first vulnerability occurs because the Mac OS X version of the `passwd` utility accepts options specifying which password database to operate on. The `passwd` binary does not check that the user has permissions to create a file in the location specified and does not set the created file permissions. By setting the file creation mask to 0 a user can create arbitrary files owned by root, with permissions which allow any user to change the contents.

The second vulnerability exists in the insecure creation of temporary files with predictable names. The temporary filename created by the process is in the form `/tmp/.pwtmp.<pid>` where `<pid>` is the process id of the `passwd` process. By creating a symbolic link to the target file, and then changing the password, it is possible to put controllable contents into the target file.

III. ANALYSIS

Successful exploitation of either of these vulnerabilities would allow a local attacker to gain elevated privileges in a number of ways.

In the case of the first vulnerability, a new file could be created in the /etc directory, such as etc/rc.local_tuning, which is sourced if it exists during the system start up process as the root user.

The second vulnerability would allow an attacker overwrite a file with user controlled contents. This can be leveraged to provide privilege escalation by, for example, creating a new /etc/sudoers file.

IV. DETECTION

iDefense has confirmed the existence of this vulnerability in Mac OS X Version 10.3.9. In addition, the following versions been confirmed by the vendor to be vulnerable:

- * Mac OS X Server Version 10.3.9
- * Mac OS X Version 10.4.5
- * Mac OS X Server Version 10.4.5

It is suspected that all prior releases are vulnerable.

V. WORKAROUND

Remove the setuid bit from the /usr/bin/passwd binary by executing the following command as root:

```
chmod -s /usr/bin/passwd
```

This workaround will prevent non-root users from being able to change their password.

VI. VENDOR RESPONSE

Apple have released an update for this vulnerability, details of which are available at the following location:

<http://docs.info.apple.com/article.html?artnum=61798>

Apple security updates are available via the Software Update mechanism:

<http://docs.info.apple.com/article.html?artnum=106704>

Apple security updates are also available for manual download:

<http://www.apple.com/support/downloads>

VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the following names to these issues:

CVE-2005-2713 – passwd file creation and permissions

CVE-2005-2714 – temporary file symlink problem

VIII. DISCLOSURE TIMELINE

08/23/2005 Initial vendor notification

08/27/2005 Initial vendor response

03/02/2006 Coordinated public disclosure

IX. CREDIT

Discovery of these vulnerabilities are credited to vade79.

Get paid for vulnerability research

<http://www.idefense.com/poi/teams/vcp.jsp>

Free tools, research and upcoming events

<http://labs.idefense.com>

X. LEGAL NOTICES

Copyright (c) 2006 iDefense, Inc.

Permission is granted for the redistribution of this alert electronically. It may not be edited in any way without the express written consent of iDefense. If you wish to reprint the whole or any part of this alert in any other medium other than electronically, please email customerservice@xxxxxxxxxxxxx for permission.

Disclaimer: The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.