

# [NEWS] Apple Mac OS X File Rewrites and Privilege Escalation

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00010.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 6 Mar 2006 13:01:44 +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>

-----

## Apple Mac OS X File Rewrites and Privilege Escalation

---

### SUMMARY

Improper handling of file permissions allows attackers to rewrite file content on Apple Mac OS X.

### DETAILS

#### Vulnerable Systems:

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

#### BOMArchiveHelper:

"BOMArchiveHelper is the default archive file handler in Mac OS X. It is a service application that has no GUI when double-clicked, rather it is invoked by opening its associated files or by choosing "Create archive of 'file'" in the Finder's File or contextual menu. It is located in /System/Library/CoreServices/BOMArchiveHelper.app," or by using safari.

A specially crafted archive utilizing a Directory Traversal in

## [NEWS] Apple Mac OS X File Rewrites and Privilege Escalation

BOMArchiveHelper allows attackers to rewrite existing files and gain root privileges by executing arbitrary programs.

Exploitation could allow a remote attacker to overwrite a file with user-supplied contents. This can be leveraged to gain code execution on the target machine by overwriting executable files such as login scripts.

Workaround:

To prevent exploitation from occurring through the Safari web browser, disable the 'Open safe file types' option in Safari. To achieve this, within Safari choose Preferences, then choose General, then uncheck the 'Open safe file types' option.

passwd file:

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

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.

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.

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.

## [NEWS] Apple Mac OS X File Rewrites and Privilege Escalation

### Vendor Status:

Apple has released Security Update 2006-001 to address the BOMArchiveHelper Directory Traversal vulnerability:

<<http://docs.info.apple.com/article.html?artnum=303382>>  
<http://docs.info.apple.com/article.html?artnum=303382>

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

<<http://docs.info.apple.com/article.html?artnum=61798>>  
<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>>  
<http://docs.info.apple.com/article.html?artnum=106704>

Apple security updates are also available for manual download:

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

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0391>>  
CVE-2006-0391  
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2713>>  
CVE-2005-2713  
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2714>>  
CVE-2005-2714

### Disclosure Timeline:

08/23/2005 Initial vendor notification  
08/27/2005 Initial vendor response  
03/02/2006 Coordinated public disclosure

### ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idefense@xxxxxxxxxxxxxxxxxxxx>> iDEFENSE Labs.

The original article can be found at:

<<http://www.idefense.com/intelligence/vulnerabilities/display.php?id=399>>  
<http://www.idefense.com/intelligence/vulnerabilities/display.php?id=399>,  
<<http://www.idefense.com/intelligence/vulnerabilities/display.php?id=400>>  
<http://www.idefense.com/intelligence/vulnerabilities/display.php?id=400>

=====

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@xxxxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxxxxx)

=====  
=====

**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.