

# [NEWS] MacOS X SoftwareUpdate Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0066.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 07/14/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Sun, 14 Jul 2002 10:03:21 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

MacOS X SoftwareUpdate Vulnerability

---

## SUMMARY

Mac OS X includes a software updating mechanism "SoftwareUpdate". Software update, when configured by default, checks weekly for new updates from Apple. HTTP is used with absolutely no authentication. Using well-known techniques, such as DNS Spoofing, or DNS Cache Poisoning it is trivial to trick a user into installing a malicious program posing as an update from Apple.

## DETAILS

### Impact:

Apple frequently releases updates, which are all installed as root.

Exploiting this vulnerability can lead to root compromise on affected systems. These are known to include Mac OS 10.1.X and possibly 10.0.X.

### Solution:

Patch is now available from apple:

<[http://download.info.apple.com/Mac\\_OS\\_X/061-0074.20020712/2z/SecurityUpdate7-12-02.dmg.bin](http://download.info.apple.com/Mac_OS_X/061-0074.20020712/2z/SecurityUpdate7-12-02.dmg.bin)>  
[http://download.info.apple.com/Mac\\_OS\\_X/061-0074.20020712/2z/SecurityUpdate7-12-02.dmg.bin](http://download.info.apple.com/Mac_OS_X/061-0074.20020712/2z/SecurityUpdate7-12-02.dmg.bin) (The patch includes cryptographic signatures on packages)

Securiteam: [NEWS] MacOS X SoftwareUpdate Vulnerability

Exploit:

A detailed way of exploiting this issue is available via:

<<http://www.cunap.com/~hardingr/projects/osx/exploit.html>>

<http://www.cunap.com/~hardingr/projects/osx/exploit.html>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:hardingr@ucsub.colorado.edu>>

Russell Harding.

=====

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@securiteam.com](mailto:list-unsubscribe@securiteam.com)

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

=====

=====

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.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[TOOL] TESO Burneye Unwrapper"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)