

Securiteam: [NEWS] MacOS X DirectoryService Privilege Escalation and DoS Attack

[NEWS] MacOS X DirectoryService Privilege Escalation and DoS Attack

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-04/0021.html>

From: support@securiteam.com

Date: 04/18/03

From: support@securiteam.com

To: list@securiteam.com

Date: 18 Apr 2003 12:30:45 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

MacOS X DirectoryService Privilege Escalation and DoS Attack

SUMMARY

DirectoryServices is part of the MacOS X information and authentication subsystem. It is launched at startup, setuid root and installed by default. It is vulnerable to several attacks ultimately allowing a local user to obtain root privileges.

DETAILS

Vulnerable systems:

- * MacOS X (10.2.4 and below)

Immune systems:

- * Mac OS X 10.2.5

During the startup of DirectoryService, the application creates a lock file by executing the touch(1) UNIX command. It executes touch through the system() libc function. This function is inherently insecure and its use is strongly discouraged in privileged applications.

Securiteam: [NEWS] MacOS X DirectoryService Privilege Escalation and DoS Attack

Since this call to system() does not specify a full path to the touch(1) command, it is possible for an attacker to modify the PATH environment variable to specify a directory containing her own version of the touch(1) command. In this instance, this would cause DirectoryService to execute arbitrary commands as root.

In order for an attacker to exploit this vulnerability, they must first cause DirectoryServices to terminate. This can be done by simply connecting to port 625 repeatedly using an automated program.

Timeline:

03/25/2003 Apple notified via email.

03/28/2003 Apple verified.

04/10/2003 Coordinated release.

Vendor Response:

"Directory Services: Fixes CAN-2003-0171 DirectoryServices Privilege Escalation and DoS Attack. DirectoryService is part of the Mac OS X and Mac OS X Server information services subsystem. It is launched at startup, setuid root and installed by default. It is possible for a local attacker to modify an environment variable that would allow the execution of arbitrary commands as root. Credit to Dave G. from @stake, Inc. for the discovery of this vulnerability."

@stake Recommendation:

@stake recommends that user upgrade to Mac OS X 10.2.5.

ADDITIONAL INFORMATION

The original advisory can be downloaded from:

<www.atstake.com/research/advisories/2003/a041003-1.txt>

www.atstake.com/research/advisories/2003/a041003-1.txt

The information has been provided by <<mailto:daveg@atstake.com>> Dave G. of @Stake.

=====

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

In order to subscribe to the mailing list, simply forward this email to: 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.