

[NEWS] MacOS X TruBlueEnvironment Privilege Escalation Attack

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-02/0028.html>

From: support@securiteam.com

Date: 02/15/03

From: support@securiteam.com

To: list@securiteam.com

Date: 15 Feb 2003 21:11:50 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

MacOS X TruBlueEnvironment Privilege Escalation Attack

SUMMARY

TruBlueEnvironment is part of the MacOS Classic Emulator. It is setuid root and installed by default. By setting certain environment variables, it is possible to overwrite any file on the system, or create arbitrary files owned as root with the attacker's umask. This vulnerability can be leveraged to create files that will be executed by root through the cron facility.

DETAILS

Vulnerable systems:

* MacOS X version 10.2.3 and below

TruBlueEnvironment uses an environment variable to determine where to write out debugging information. Local users can set this to environment variable to point at any file on the file system. If the file exists, it will be reset to zero bytes. If the file does not exist, it will be created with the umask inherited from the calling process. While attackers cannot create files with execute permissions set, they can create files that are world writable.

Securiteam: [NEWS] MacOS X TruBlueEnvironment Privilege Escalation Attack

Under MacOS X, this vulnerability can be used to create files that will be run automatically via cron. By default, cron will launch maintenance scripts using the periodic command. This command will take several files and either 'source' them or run them through a shell interpreter. Since these scripts are running as root, it is possible to obtain administrator privileges on any MacOS X system running cron and TruBlueEnvironment.

Vendor Response:

Classic: The Mac OS X 10.2.4 release fixes CAN-2003-0088, where an attacker may change an environment variable to create arbitrary files or overwrite existing files, which could lead to obtaining elevated privileges. Credit to Dave G. from @stake, Inc. for discovering this issue.

Recommendation:

If possible, upgrade to Mac OS X 10.2.4. Another solution is to restrict access to the TruBlueEnvironment (*) executable, or remove it entirely if it is not being used. One approach to restricting access would be to remove global execute permissions from the TruBlueEnvironment executable, and only allow a specific group to execute the application. The following commands will restrict access to the 'admin' group:

```
sudo chown .admin /System/Library/CoreServices/Classic\
Startup.app/Contents/Resources/TruBlueEnvironment
```

```
sudo chmod 4750 /System/Library/CoreServices/Classic\
Startup.app/Contents/Resources/TruBlueEnvironment
```

(*) Located in /System/Library/CoreServices/Classic
Startup.app/Contents/Resources/TruBlueEnvironment

ADDITIONAL INFORMATION

The original advisory can be downloaded from:

<<http://www.atstake.com/research/advisories/2003/a021403-1.txt>>
<http://www.atstake.com/research/advisories/2003/a021403-1.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

=====
=====

Securiteam: [NEWS] MacOS X TruBlueEnvironment Privilege Escalation Attack

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.