

[NEWS] Aborting the OS X's Init Script Allows Gaining of Root Console

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0025.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/04/03

To: list@securiteam.com

Date: 4 Nov 2003 15:54:11 +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>

Aborting the OS X's Init Script Allows Gaining of Root Console

SUMMARY

Mac OS X's Init script can be crashed by holding down the CTRL-C keys on a USB keyboard. Once the Init script has crashed enough times, it will drop the user into a root console.

DETAILS

Vulnerable systems:

- * Mac OS X version 10.2.7 and prior
- * Mac OS X version 10.2.8

Immune systems:

- * Mac OS X version 10.3.0

Mac OS X's Init script can be crashed using a USB keyboard by holding down CTRL-C immediately after boot, and keeping it held down. Init will crash two or three minutes into the boot process which will be followed by it dropping into a root shell.

At this point, you can of course modify the file system, or selectively

Securiteam: [NEWS] Aborting the OS X's Init Script Allows Gaining of Root Console

run components of the rc scripts to bring up full OS X functionality without the GUI layer, which will demand a root password and lock you out once its spawned successfully.

The 'exploit' is dependant on a USB keyboard being used. It will not work on a PowerBooks without a USB keyboard attached, for example.

Vendor status:

This was originally reported to Apple in 1998, and Jason was informed that this was an 'internal development feature' that would be removed.

Three years later Jason reported this 'internal development feature' again, and received no reply at all.

Now that Panther is out and this 'internal development feature' appears to be resolved (no doubt thanks to the massive reworking of OS X USB code), Jason sees no reason not to give people a good reason to upgrade by releasing this information.

ADDITIONAL INFORMATION

The information has been provided by <mailto:jms@lasergun.org> Jason Storm.

=====

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.