

RE: Mounting filesystems with "noexec"

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-09/0024.html>

From: Rob MacGregor (freebsd.macgregor_at_blueyonder.co.uk)

Date: 09/22/05

To: <freebsd-security@freebsd.org>

Date: Thu, 22 Sep 2005 12:24:46 +0100

On Thursday, September 22, 2005 12:12 PM, Borja Marcos <> unleashed the infinite monkeys and produced:

- > *First thing, an attempt to execute a program from a noexec-mounted*
- > *filesystem should be logged. It is either a very significant security*
- > *event, or it can drive nuts an administrator trying to install*
- > *software. (I like to mount with noexec filesystems such as /var, /var/*
- > *www, /var/spool, /var/tmp, /tmp, /home whenever the users are not*
- > *supposed to install software...).*

As long as you can disable/limit the logging. One very nasty "attack" would be to loop trying to run a binary. Blow your logging partition. Somebody could then use that to do other things that would normally be logged, safe in the knowledge that their activities wouldn't be logged.

I've seen systems brought to their knees by similar well intentioned logging activities. It's not pretty :)

--

Rob | Oh my God! They killed init! You bastards!

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"