

Re: Mounting filesystems with "noexec"

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-09/0035.html>

From: Borja Marcos (borjamar_at_sarenet.es)

Date: 09/23/05

Date: Fri, 23 Sep 2005 09:05:13 +0200
To: Andreas Jonsson <andreas@romab.com>

> *Instead of running "./script.sh" or "./script.pl" you just have to*
> *type*
> */bin/sh script.sh or /usr/bin/perl script.pl which gives pretty much*
> *everything you need when it comes to using exploits. In linux you*
> *could*
> *also circumvent it by using /lib/ld.so exploit, but i'm not sure if*
> *that*
> *is "fixed" now or not.*

I'm well aware of this, obviously :-)

But, with TPE or without TPE, any command with a script language, be it a shell, Perl, Tcl, or whatever (even Java) should perform that check, which is not a good design practice.

That said, my point is this: the amount of damage you can do from a "native" program is greater than the damage you can achieve from a script language, afaik. At least a privilege escalation should be harder to obtain. I'm not sure about some languages such as Perl, though.

Of course, this is only one among a bigger set of security measures.

Borja.

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"