

Re: RFC: Removing file(1)+libmagic(3) from the base system

# Re: RFC: Removing file(1)+libmagic(3) from the base system

---

*Source:* <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/arch/2007-05/msg00150.html>

---

- *From:* Kris Kennaway <[kris@xxxxxxxxxxxxxxxx](mailto:kris@xxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 23 May 2007 21:17:48 -0400
- 

On Wed, May 23, 2007 at 05:55:35PM -0700, Julian Elischer wrote:

Colin Percival wrote:

Poul-Henning Kamp wrote:

In message <46546E16.9070707@xxxxxxxxxxxx>, Colin Percival writes:

I'd like to remove file(1) and libmagic(3) from the FreeBSD base system for the following reasons:

One mitigating option would be to open the magic file and input and sequester the file process in a jail.

Last time I checked, unprivileged processes couldn't jail themselves. We could make file(1) setuid root and use a privilege separation approach, but I'm not convinced that would be a net win.

How about a bit in the headers of a program that are set by the Makefile. If the bit is not set then the elf program executor sets a bit that forbids exec from ever running..

how many programs actually need to be able to run exec..  
the average exploit does an exec(/bin/sh)

Cart before horse. Colin needs to first tell us what attack he is trying to stop before we can figure out how to stop it.

Kris

P.S. Thesedays we have the MAC subsystem, no need for magic hacks of this nature.

Re: RFC: Removing file(1)+libmagic(3) from the base system

Re: RFC: Removing file(1)+libmagic(3) from the base system

---

freebsd-arch@xxxxxxxxxxx mailing list

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

To unsubscribe, send any mail to "freebsd-arch-unsubscribe@xxxxxxxxxxx"