

Re: dlopen(), atexit() crash on FreeBSD (testcase included)

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/hackers/2007-12/msg00290.html>

- *From:* Jason Evans <jasone@xxxxxxxxxxxx>
 - *Date:* Mon, 31 Dec 2007 11:32:03 -0800
-

Markus Hoenicka wrote:

I've been redirected by Giorgos Keramidas to this list after reporting a problem on the freebsd-questions list. I'd greatly appreciate if you could have a look at the following problem. Apparently programs are doomed to segfault on FreeBSD if dlopen()ed modules install exit handlers via atexit(). Similar problem reports have cropped up before,

It seems to me that you should *expect* a crash under the circumstances you describe. You are dlopen()ing a module, saving a pointer to a function within that module, unloading the module, then trying to call a function that is no longer mapped. The only way this could possibly work is if dlclose() doesn't really unmap the module. It is up to the programmer to avoid dangling pointers to unmapped modules. There are all sorts of variations on this bug, such as storing a pointer to a const string. You have to be really careful to be able to safely dlclose() a module.

Jason

freebsd-hackers@xxxxxxxxxxxx mailing list

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

To unsubscribe, send any mail to "freebsd-hackers-unsubscribe@xxxxxxxxxxxx"