

[CFT] NDIS optional header length related fixups

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/current/2005-06/1422.html>

From: Andrew R. Reiter (arr_at_watson.org)

Date: 06/29/05

Date: Wed, 29 Jun 2005 15:06:52 -0400 (EDT)

To: freebsd-current@FreeBSD.org

Calling NDIS -CURRENT users,

Attached is a patch that should fix any possible issues with mis-calculating offsets or sizes when dealing with anything 'image_optional_header' related in the PE loading code. The reason for the patch is that the optional header can have a varying length due to the lack of requiring the existence of all the 'image_data_directory's to exist within a binary. As far as I can tell, most drivers tend to include all, but due to the basic idea that there can be less than IMAGE_DIRECTORY_ENTRIES_MAX data directories in the optional header, we should at least make an attempt at preemptively catch any bugs that might arise due to improper pointer calculation.

If you could, please give it a run in your tree!

The patch is also located at:

http://www.watson.org/~arr/ndis_opthdrsz.diff

I guess let me know if anyone has any problems with this working (or other).

Cheers,
Andrew

--

Andrew R. Reiter
arr@watson.org

freebsd-current@freebsd.org mailing list

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

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

- TEXT/PLAIN attachment: [ndis_opthdrsz.diff](#)