

Re: FreeBSD 5.1-p10 reproducible crash with Apache2

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/current/2003-10/1486.html>

From: Kris Kennaway (kris_at_obsecrity.org)

Date: 10/30/03

Date: Wed, 29 Oct 2003 21:05:40 -0800

To: "Branko F. Gra?nar" <bfgr@noviforum.si>

On Wed, Oct 29, 2003 at 11:37:56AM +0100, "Branko F. Gra?nar" wrote:

> *Hi.*

>

> *FreeBSD 5.1-p10 (and also possible other 5.1-pX version) can be remotely
> locked up if the following criteria is met:*

>

> + *apache2 has mod_ssl loaded and enabled*

> + *apache2 has the following configuration directives set to the
> following values:*

>

> *SSLMutex sem*

> *SSLSessionCache shm:/some/file(1048576)*

>

> + *client connects via SSL/TLS to apache fast enough.*

>

> *If all conditions above are satisfied except the last one, then lockup
> doesn't happen.*

>

> *I tested on three 5.1-p10 machines (SMP, uniprocessor, uniprocessor with
> hypterthreading) with JMeter 1.9.1.*

>

> *It is possible lockup machine with 100 requests (1 concurrent request)
> in 1-3 seconds.*

>

> *If SSLMutex is set to file:/path/somewhere and SSLSessionCache is set to
> dbm:/some/dbm lockup does not accour.*

>

> *Linux 2.4.22 is not affected by this issue.*

>

> *Details:*

What kernel configuration? What hardware?

Kris

- application/pgp-signature attachment: stored