

Re: FreeBSD Security Advisory FreeBSD-SA-05:09.htt [REVISED]

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-05/0031.html>

From: David Schultz (*das_at_FreeBSD.ORG*)

Date: 05/13/05

Date: Fri, 13 May 2005 12:07:14 -0400

To: freebsd-security@FreeBSD.ORG

On Fri, May 13, 2005, FreeBSD Security Advisories wrote:

> *II. Problem Description*

>

> *When running on processors supporting Hyper-Threading Technology, it is possible for a malicious thread to monitor the execution of another thread.*

>

> *NOTE: Similar problems may exist in other simultaneous multithreading implementations, or even some systems in the absence of simultaneous multithreading. However, current research has only demonstrated this flaw in Hyper-Threading Technology, where shared memory caches are used.*

But isn't this a well-known and fundamental problem with SMT?

Someone at Sun pointed out a similar attack to me in 2003; it turns out that it's possible for a thread to monitor which of the processor's functional units another thread is using. For instance, you can sample the number of shifts vs. adds vs. multiplies and use this information to mount a differential timing attack. Also, recent work [1] shows that programs with key-dependent cache behavior can be attacked even without SMT. So this sounds like trying to solve in the OS a problem that can only be solved in the application. Is there something more subtle that's going on?

P.S. I'm getting on a plane in a few hours, and I may be unable to respond for a few days.

[1] <http://cr.yp.to/antiforgery/cachetiming-20050414.pdf>

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"