

Re: [Full-disclosure] Cisco IOS Shellcode Presentation

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-07/0699.html>

From: Andrew R. Reiter (arr_at_watson.org)

Date: 07/29/05

Date: Fri, 29 Jul 2005 16:03:01 -0400 (EDT)

To: Tim <tim-security@sentinelchicken.org>

On Fri, 29 Jul 2005, Tim wrote:

:> How about adopting an architecture that incorporates special-purpose
:> security safeguards into the CPU? Routers and switches don't need to
:> execute arbitrary code, Cisco knows ahead of time, before they deploy a
:> product, what code that product should be allowed to execute.

:>

:> Do you think there is no way in hardware to limit the code that gets
:> executed? Maybe you should join the FBI.

:

:Hardware has bugs too.

:

:Arbitrary code execution isn't too hard on the XBox, for instance, even
:with complex crypto checks.

:

:Intel screwed up their design of hyperthreading with caches, and as a
:result, local users can steal data from one another.

Intel did? How's that? This cache issue has been a problem before at different levels. You're stating that it's the CPU's job to determine scheduling of what threads are running on the HTT enabled CPU. Do you want another cache for each 'virtual' cpu? Sounds like you might just want to go the next step and do a true MP system instead of virtual :). I'd blame the OS scheduler before Intel with regards to this cache issue.

:

:I think your broad suggestion is flawed. Perhaps the only reason we
:*don't* see as many hardware-based bugs, is that when you are getting
:ready to put something in hardware, you are generally more interested in
:getting it right the first time, given the production costs. The
:problem is, the mode of failure is astronomically worse, as you can't
:easily patch any problems that do crop up.

I agree and disagree, I think if there were folks (kiddies) out there who could understand hardware design in & out's like they do PHP scripting,

Full-Disclosure: Re: [Full-disclosure] Cisco IOS Shellcode Presentation

you'd find that there might be more bugs published in that arena.
However, your point regarding "getting it right" is a good one... cost is key when doing hardware, so ensuring things are done "right" in the beginning is key.

:

:On another note:

:The unfortunately common misconception that 'appliances' are safe
:because they are "hardware devices" really needs to go. Everything is a
:combination of hardware and software, and that's how it should be, from
:an engineering perspective.

:

:>From a security perspective, software should be viewed as a living thing
:that constantly needs feeding, whether it is on a funny-looking
:rackmount proprie