

# Re: Public disclosure of discovered vulnerabilities

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-06/0397.html>

---

*From:* David Wagner ([daw\\_at\\_taverner.cs.berkeley.edu](mailto:daw_at_taverner.cs.berkeley.edu))

*Date:* 06/07/05

Date: Tue, 7 Jun 2005 09:16:43 +0000 (UTC)

John E. Hadstate wrote:

> "David Wagner" <[daw@taverner.cs.berkeley.edu](mailto:daw@taverner.cs.berkeley.edu)> wrote:  
>> *heap exploits,*  
>> *return-into-libc buffer overruns, GOT table overruns, NOP*  
>> *landing pads, [...]*  
>> *format string vulnerabilities, integer overflow*  
>> *vulnerabilities, double-free vulnerabilities, [...]*  
>  
> *I don't know what "people" understood, but I experimented*  
> *with, experienced and understood all of them more than 20*  
> *years ago.*

I confess I'm pretty surprised to see you write that. Do you really mean what you wrote? If so, I'm stunned and truly impressed. What can I say? I guess you were a decade or more ahead of the rest of us.

I've followed the state of the art in buffer overrun exploitation. I remembered when many of these new methods were first discovered and revealed to the public, and they were not obvious at the time. I remember the bugtraq posts and exploit code that first revealed most of these methods. I am quite certain that it was a lot more recently than 20 years ago: if I can remember when they were first discovered, that was certainly less than 20 years ago.

(Actually, NOP landing pads might be very old -- I don't know about that one. But I think the other buffer overrun methods are quite recent. There was a time when most people thought that stack overruns were pretty much the only kind of overrun worth worrying about.)

Likewise, the discovery that double-free bugs and format string bugs could be exploited to take over your machine was quite recent -- in the past decade.

If you were fully aware of these attack techniques 20 years ago, well, gee, you were lightyears ahead of what was publicly known at the time. I can tell you that there was no public knowledge of this stuff 20 years ago. I can tell you that there was no understanding of this in the security community 20 years ago. If anyone knew of all these attack

sci.crypt: Re: Public disclosure of discovered vulnerabilities

methods 20 years ago, they weren't talking. I wish we'd known about this 20 years ago...

Do I need to dig up citations to the first known public description of these attacks, to convince you that this wasn't known to the public community 20 years ago? I'm a bit reluctant to go to the work, but I'll give it a try if you really want.