

## Re: Scanners and unpublished vulnerabilities – Full Disclosure

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-05/0099.html>

---

**From:** Ryan Russell ([ryan@securityfocus.com](mailto:ryan@securityfocus.com))

**Date:** 05/28/02

Date: Tue, 28 May 2002 14:00:16 -0600 (MDT)  
From: Ryan Russell <[ryan@securityfocus.com](mailto:ryan@securityfocus.com)>  
To: Alfred Huger <[ah@securityfocus.com](mailto:ah@securityfocus.com)>

On Tue, 28 May 2002, Alfred Huger wrote:

> *jumping to a visceral conclusion one way or another. The way this impacts*  
> *the Pen-testing community is that these vulnerabilities which are in the*  
> *process (presumably) of being fixed are actively being coded into the*  
> *Typhon II Vulnerability Assessment Scanner from NGSSoftware.*

I would suspect this wouldn't have much of an impact on the pen-testing community, but I'll leave it to the professional pen-testers to answer how often the very latest vulnerabilities come into play in their work. My experience comes more from seeing how often really, really old vulnerabilities are used in the wild, and work. This would tend to have to also partially reflect the companies that hire pen-testers, though if they've taken the step to hire someone, that company is at least demonstrating a little more clue.

What it boils down to is the rest of us will have the information, just a little later. I suppose part of the controversy is that NGSSoftware is presumably going to benefit from holding back information, i.e. if you want to check for the vulns they found, you have to buy their product. This isn't new, either. A few years ago at a previous employer, I was a licensed user of ISS' Internet Scanner. They had a check for a statd bug (which came to my attention because it was getting positive matches) that I could find no public documentation on. I.e. I was doing an internal penetration test, and having a potential hole, I wanted to go ahead and exploit it fully.

Of course the punchline is that I simply pulled out a sniffer, and read the vulnerability details off the wire (it's was a simple .. bug.) So, NGSSoftware customers have full access to the details, no surprise. It should