

# [Full-disclosure] Re: Publishing exploit code – what is it good for

**Source:** <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-06/0425.html>

---

**From:** Damian Menscher (*mensch\_ at \_uiuc.edu*)

**Date:** 06/30/05

Date: Thu, 30 Jun 2005 15:08:57 -0500 (CDT)

To: bugtraq@securityfocus.com

On Thu, 30 Jun 2005, Aviram Jenik wrote:

- > *What I need is a security administrator, CSO, IT manager or sys admin that can*
- > *explain why they find public exploits are good for THEIR organizations. Maybe*
- > *we can start changing public opinion with regards to full disclosure, and*
- > *hopefully start with this opinion leader.*

I'll skip over the obvious stuff (exploits are distributed anyway, knowing when exploits exist is helpful for prioritizing patches, etc) and jump to your specific question: how this helps me and my organization as end-users.

When a vendor issues an advisory, it tells us that their software should be upgraded, and often gives mitigating factors. But upgrading software all the time is risky: you never know when a patch will break something. So it's often helpful to wait a day before upgrading, if you know that there is no known exploit. FD lists therefore help us prioritize updates.

Also, many times there are enough mitigating factors that it may be difficult to determine whether (in the case of an exploit being published before we've had a chance to patch) there was any period of vulnerability. For example, with stack randomization enabled, the exploit might fail. It would be reassuring to confirm that.

Finally, many vendors (RedHat being a notable one) backport security patches, rather than upgrading to the latest version (which may introduce new bugs^Wfeatures). A side effect is that it's often difficult to determine whether your machines are vulnerable to any given exploit. Yes, we could probably glean the information from changelogs and security advisories from the vendor, but that's often a confusing process (the inclusion of CAN/CVE numbers helps).

And, of course, if you're the security guy (I've worn this hat too), all you can see is that they're running (for the case of OpenSSH)

Full-Disclosure: [Full-disclosure] Re: Publishing exploit code – what is it good for

OpenSSH\_3.6.1p2, which might be vulnerable. You don't know that the fix was backported into openssh-3.6.1p2-33.30.4. So you need to test. In fact, I suspect this is why your friend doesn't want the exploits to be released. If organizations could test their own security (which \*requires\* having the exploits, as I just explained), it would cut into his company's market-share.

Damian Menscher

--

```
--#| Physics Grad Student & SysAdmin @ U Illinois Urbana-Champaign |#=-  
--#| 488 LLP, 1110 W. Green St, Urbana, IL 61801 Ofc:(217)333-0038 |#=-  
--#| 4602 Beckman, VMIL/MS, Imaging Technology Group:(217)244-3074 |#=-  
--#| <menscher@uiuc.edu> www.uiuc.edu/~menscher/ Fax:(217)333-9819 |#=-  
--#| The above opinions are not necessarily those of my employers. |#=-
```

---

Full-Disclosure - We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia - <http://secunia.com/>