

## RE: Pubstro rash

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2005-03/0045.html>

---

**From:** k levinson ([levinson\\_k\\_at\\_yahoo.com](mailto:levinson_k_at_yahoo.com))

**Date:** 03/17/05

Date: Thu, 17 Mar 2005 14:09:40 -0800 (PST)

To: [incidents@securityfocus.com](mailto:incidents@securityfocus.com)

> -----Original Message-----

> *From: David Gillett [mailto:[gillettdavid@fhda.edu](mailto:gillettdavid@fhda.edu)]*

> *3. Instead of a random high port, the installed FTP server*

> *listens on port 53. Which I can't block, because DNS may*

> *need to use it, right?*

No. Destination ports TCP/UDP 53 should not be allowed inbound to your workstations. Dest ports TCP/UDP 53 are only needed in to your network if you have your own DNS server for resolution of your own domain names by clients on the Internet, and then it should only be to your DNS server. It sounds like your firewall rules could use some inspection.

Said another way, the rule on your firewall that permits Internet hacker:port x -> your network:port 53 is a different than the rule that permits your clients:x -> Internet DNS:53, and blocking the former rule should have no effect on your internal clients accessing Internet DNS.

You may also seriously want to consider setting up your own DNS server, even a Windows one, so that no clients can send outbound to dest port TCP/UDP 53 to the Internet, only your DNS server. A proxy server or firewall that proxies is a possibility as well, to try to ensure that port 53 traffic is DNS and not something else being tunneled.

Using NAT between your workstations and the Internet might have prevented some or all of this, if it is possible to do this in your environment.

SecurityFocus Incidents: RE: Pubstro rash

- > 5. *At this point, I don't know how the machines are getting*
- > *compromised initially. I'd appreciate if anyone else is seeing*
- > *this pattern and has some insight they'd care to share.*

These things are usually because of something well known, such as a missing patch, or via a security problem that has nothing to do with a patch, like a bad password or poorly configured settings. You can of course run MBSA from Microsoft to find what patches are missing, free from [www.microsoft.com/mbsa](http://www.microsoft.com/mbsa). If MBSA states that all patches are installed, then it might be fruitful to hypothesize about other possible vectors. Knowing what ports are open inbound to the workstations and what if anything up to date AV scanners showed might be useful too.

– Karl

---

Do you Yahoo!?

Yahoo! Small Business – Try our new resources site!

<http://smallbusiness.yahoo.com/resources/>