

Full-Disclosure: [Full-Disclosure] RE: SQL Slammer doing the rounds again?

[Full-Disclosure] RE: SQL Slammer doing the rounds again?

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-11/0673.html>

From: Jim Harrison (ISA) (jmharr_at_microsoft.com)

Date: 11/14/03

To: <nick@virus-1.demon.co.uk>, <incidents@securityfocus.com>

Date: Thu, 13 Nov 2003 15:42:23 -0800

(hee-hee); nice shots..

> *Isn't "should" kind of a "maybe"?? 8-*

..Yep, I was assuming that this was the only reason the poor netadmin had to allow access to the SQL over TCP-1434. My bad...

RE: the web designers and their choices; I can't speak to the issues (really; I don't know them) regarding my own company's design choices, but I'll bet they'd love to hear from you directly.

The idea of "listen to the customer" is being made very clear to everyone these days.

The "squeaky wheel..." and all that.

* Jim Harrison

MCP(NT4/2K), A+, Network+
Security Business Unit (ISA SE)

"I used to hate writing assignments, but now I enjoy them.

I realized that the purpose of writing is to inflate weak ideas, obscure poor reasoning, and inhibit clarity.

With a little practice, writing can be an intimidating and impenetrable fog!"

-Calvin

-----Original Message-----

From: Nick FitzGerald [<mailto:nick@virus-1.demon.co.uk>]

Sent: Thursday, November 13, 2003 14:56

To: incidents@securityfocus.com

Cc: Jim Harrison (ISA); Harlan Carvey; full-disclosure@lists.netsys.com

Subject: RE: SQL Slammer doing the rounds again?

"Jim Harrison (ISA)" <jmharr@microsoft.com> replied to "Harlan Carvey" <keydet89@yahoo.com>:

[corrected for top-postingitis]

[Full-Disclosure] RE: SQL Slammer doing the rounds again?

Full-Disclosure: [Full-Disclosure] RE: SQL Slammer doing the rounds again?

> > *While I fully agree w/ Jim's advice, one thing I'm*
> > *still curious about...since we first saw Slammer...is*
> > *this – Is there a valid business reason to expose UDP*
> > *1434 to the Internet?*
> >
> > *I've asked this before and not received any responses.*
> >
> > *If anyone has one, I'd love to hear it. Please*
> > *refrain from the "maybes"...I'd like to hear valid*
> > *reasons why this port is exposed.*
>
> *The simple answer is, "if the web app is properly designed, coded and*
> *tested, there should be no reason to 'open a port' (apologies to TS)*
to