

Re: bugtraq inetd DoS exploit *PFFT*

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2001-02/1267.html>

From: Nick Slager (nicks@albury.net)

Date: 02/27/01

Date: Tue, 27 Feb 2001 11:51:51 +1100
From: Nick Slager <nicks@albury.net>
To: Marius Strom <marius@marius.org>

Thus spake Marius Strom (marius@marius.org):

>On Tue, Feb 27, 2001 at 10:50:17AM +1100, Nick Slager wrote:

>>

>> *The inetd shipped with FreeBSD appears vulnerable to the inetd DoS*

>> *exploit posted on bugtraq.*

>>

>> ...

>>

>> *As a workaround, start inetd with the -C flag.*

>

> *This is not a "vulnerability", per se. inetd(8) will suspend a service*

> *for 10 minutes if a certain amount of them are started within a certain*

> *time, hence your log message. Not to deny that it's a limited DoS*

> *condition, but it was programmed that way.*

>

> *To update this on a per-service basis (say, your pop3 daemon takes lots*

> *of hits under normal traffic) do the following:*

[snip inetd.conf entry and man page quote]

erm, thanks, I do realise this. The advantage of the -C flag is being able to specify the maximum times a given service can be invoked from a single IP, ensuring services are still available for other clients.

Nick

--

Nick Slager | Quidquid latine dictum
nicks@albury.net | sit, altum viditur.
To Unsubscribe: send mail to majordomo@FreeBSD.org
with "unsubscribe freebsd-security" in the body of the message