

Re: some "scanned with SSH-1.0-SSH_Version_Mapper. Don't panic." in syslog

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2001-12/0244.html>

From: Matthew D. Close (mclose@exodus.net)

Date: 12/24/01

Date: Sun, 23 Dec 2001 17:44:21 -0800 (PST)
From: "Matthew D. Close" <mclose@exodus.net>
To: Steffen Dettmer <steffen@dett.de>

The SSH-1.0-SSH_Version_Mapper is from a scanning tool called scanssh.
You can find it at <http://www.monkey.org/~provos/scanssh/>

I've seen a substantial increase in ssh scans over the last month or so.
Probably a result of the recent vulnerabilities listed on CERT.

There seem to be two types of scanning going on, one that looks like
scanssh. Then another that's a SYN scan, with a normal reconnect to port
22 if the first scan found anything open.

matthew

On Sat, 22 Dec 2001, Steffen Dettmer wrote:

>
> Hi,
>
> I found the following in syslogs on some servers (running
> OpenSSH):
>
> sshd[29575]: scanned from ::ffff:62.154.180.3 with
> SSH-1.0-SSH_Version_Mapper. Don't panic.
>
> and on nearly every server things like:
>
> sshd[13669]: connect from root@62.154.180.3
> sshd[13669]: log: Could not reverse map address 62.154.180.3.
>
> Well, just looks like a portscan. There are a lot fo them these
> days. But I have a few old SuSE hosts here. I've upgraded the
> installed SSH with the latest patches. Those hosts logged:
>
> sshd[13669]: fatal: Local: Your ssh version is too old and is no

SecurityFocus Incidents: Re: some "scanned with SSH-1.0-SSH_Version_Mapper. Don't panic." in syslog

> longer supported. Please install a newer version.
>
> Is this just a message for some unsupported protocol version (or
> if the scanner don't use any protocol string after connect)?
> Or is it anything to worry about? (Yes, complete update is
> already sheduled :))
>
> Anyway, this may be a large scan which just hit my (small)
> network.
>
> Does anyone knows somethink about SSH-1.0-SSH_Version_Mapper?
>
> BTW, merry christmas and a happy new year.
>
> oki,
>
> Steffen
>
> --
> Dieses Schreiben wurde maschinell erstellt,
> es trägt daher weder Unterschrift noch Siegel.
>
>

> This list is provided by the SecurityFocus ARIS analyzer service.
> For more information on this free incident handling, management
> and tracking system please see: <http://aris.securityfocus.com>
>

This list is provided by the SecurityFocus ARIS analyzer service.
For more information on this free incident handling, management
and tracking system please see: <http://aris.securityfocus.com>

- **Previous message:** [Kneppers: "SNMP scans, DoS and a VIP crash"](#)
- **In reply to:** [Steffen Dettmer: "some "scanned with SSH-1.0-SSH_Version_Mapper. Don't panic." in syslog"](#)
- **Next in thread:** [Jose Nazario: "Re: some "scanned with SSH-1.0-SSH_Version_Mapper. Don't panic." in syslog"](#)
- **Reply:** [Jose Nazario: "Re: some "scanned with SSH-1.0-SSH_Version_Mapper. Don't panic." in syslog"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)