

Re: Microsoft SQL Server Stored procedures [sp_MSSetServerPropert iesn and sp_MSsetalertinfo] (#NISR03092002A)

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2002-09/0005.html>

From: David Litchfield (david@NGSSOFTWARE.COM)

Date: 09/04/02

Date: Wed, 4 Sep 2002 22:44:34 +0100
From: David Litchfield <david@NGSSOFTWARE.COM>
To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

Karsten Højgaard KHojgaard@DK.SNT.COM wrote:

>> [...] It does not allow an > attacker to compromise the server or data but
may be used in conjunction > with another attack. For example an attacker
may not >want SQL Server to > restart on server reboot if they set a shell
listening on TCP port 1433.

>There's easier ways to access the port than actually halting the process.

>An application can normally listen to either a specific interface, or all
interfaces (the normal approach). A little known fact is that a process that
binds to a specific >ip silently overrides processes listening on all ips
and the same port(s).

>This can be tested by getting netcat for windows at
http://www.atstake.com/research/tools/#network_utilities, and instructing it
to listen on your public ip, e.g. on >port 80, while you run IIS or PWS.

>Not that IIS is still running, and not returning errors, while actual
connects to the machine's public ip are in fact handled by netcat.

As far as IIS is correct this is true. You can bind netcat over the port.
But if you've ever tried to bind netcat to 1433 when SQL Server is bound to
it you'll see it fails.

```
C:\sqlstuff>netstat -an
```

Active Connections

```
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1025 0.0.0.0:0 LISTENING
```

T-Bugtraq: Re: Microsoft SQL Server Stored procedures [sp_MSSetServerPropert iesn and sp_MSsetalertinfo] (#NISR030

```
TCP 0.0.0.0:1029 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1433 0.0.0.0:0 LISTENING
```

```
..
..
```

As can be seen SQL Server is not bound to a specific IP address – however:

```
C:\sqlstuff>nc -l -p 1433
Can't grab 0.0.0.0:1433 with bind
```

also

```
C:\sqlstuff>nc -l -p 1433 -s 10.1.1.37
Can't grab 10.1.1.37:1433 with bind
```

Under HKLM\System\CurrentControlSet\Services\Tcpip\parameters I have a key Reserved ports whose value is 1433–1434 1352–1352. This could be something to do with it failing with SQL Server. I haven't examined this behaviour too deeply though so don't quote me on that ;)

Cheers,
David Litchfield
NGSSoftware Ltd
<http://www.nextgenss.com/>

p.s. In the original advisory I incorrectly said drop execute for the fix – of course it should be revoke execute.

-
- **Previous message:** [Russ: "Alert: Microsoft Security Bulletin – MS02–050"](#)
 - **Maybe in reply to:** [Karsten Højgaard: "Re: Microsoft SQL Server Stored procedures \[sp_MSSetServerPropert iesn and sp_MSsetalertinfo\] \(#NISR03092002A\)"](#)
 - **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)

Re: Microsoft SQL Server Stored procedures [sp_MSSetServerPropert iesn and sp_MSsetalertinfo] (#NISR