

Re: sql 2005 vulnerability hello overflow?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2007-03/msg00149.html>

- *From:* K. Brian Kelley <brian_kelley@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sat, 24 Mar 2007 18:12:47 +0000 (UTC)
-

To piggyback on Mr. Smith, for some reason Nessus is thinking it's a SQL Server 2000 box because the following is in the NASL to test for the vulnerability:

```
version = get_kb_item("mssql/SQLVersion");
if(version)
{
if(!ereg(pattern:"^8\\.00\\.(0?[0-5][0-9][0-9]0?6[0-5][0-9]|66[0-4])",
string:version))exit(0);
}
```

Note the regex pattern which is supposed to only filter for SQL Server version 8.00.x, meaning SQL Server 2000. Your security folks can confirm this here:

<http://www.nessus.org/plugins/index.php?view=viewsrc&id=11067>

K. Brian Kelley, [brian_underscore_kelley at sqlpass dot org](mailto:brian_underscore_kelley@sqlpass.org)
<http://www.truthsolutions.com/>

we have built a new w2003 sp2, sql 2005 sp2 with hotfix server. Scanning with Nexus tells us it is vulnerable to the hello overflow, CVE-2002-1123. How can I find out for certain whether the server is vulnerable or not? need to be able to show documentation to our security guy b4 can go into production. Thanks VERY much.

The remote MS SQL server is vulnerable to the Hello overflow.

An attacker may use this flaw to execute commands against the remote host as LOCAL/SYSTEM, as well as read your database content.

*** This alert might be a false positive.

Solution : Install Microsoft Patch Q316333 at
[http://support.microsoft.com/default.aspx?scid=kb;en-us;Q316333&sd=tec](http://support.microsoft.com/default.aspx?scid=kb;en-us;Q316333&sd=tech)
h

Re: sql 2005 vulnerability hello overflow?

or disable the Microsoft SQL Server service or use a firewall to protect the

MS SQL port (1433).

Risk factor : High

CVE : CVE-2002-1123

BID : 5411

Other references : IAVA:2002-B-0007, OSVDB:10132

Nessus ID : 11067