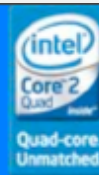




But now you can keep your network running smoothly, round the clock with...

7:54:43 PM



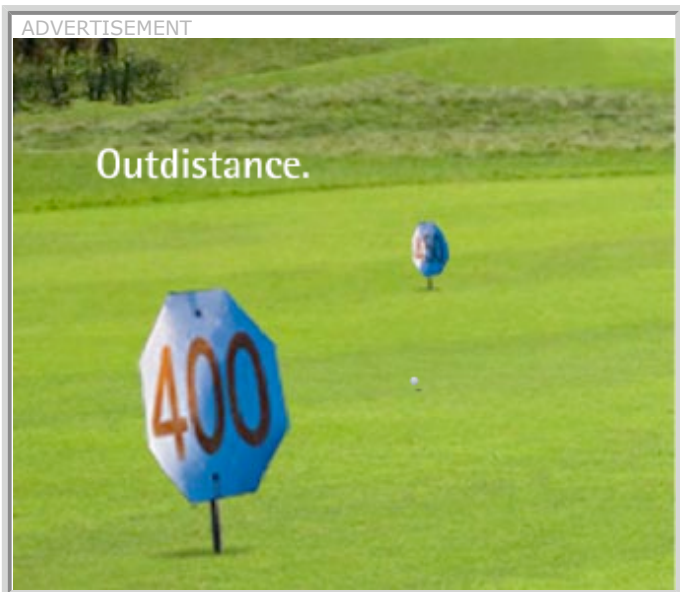
Thousands of Unprotected Databases Litter the Internet

November 14, 2007

By Lisa Vaas

After checking 1,160,000 random IP addresses, a security firm found nearly half a million database servers on the Internet not protected by firewalls—most of them were running Microsoft SQL Server, but a healthy portion of them were Oracle databases.

Next Generation Security Software released on Nov. 12 a report saying the company found 368,000 Microsoft SQL Server databases and around 124,000 Oracle database servers, all directly accessible on the Internet. Between the two vendors, there were 492,000 unprotected database servers out on the Internet without firewalls.



The findings represent a "significant risk," according to David Litchfield, the security researcher who authored the report. "With just under half a million servers accessible, there is clearly potential for external hackers and criminals to gain access to these systems and to sensitive information," he said.

- RELATED LINKS**
- [TJX's Projected Breach Costs Increase to \\$216M](#)
 - [Mozilla to Fix 9-Month-Old JAR URL Handling Bug](#)
 - [Microsoft Patches DNS, URI-Handling Flaws](#)
 - [Seagate Storage Units Ship with Virus](#)
 - [Microsoft Makes Office 2007 More Secure](#)

"It is well known that Oracle prior to 10g installs with a number of user accounts with default passwords, including DBA accounts, and earlier versions of SQL Server would install with the superuser account ... with a blank password. How many of these unprotected database servers have these

defaults in place?" Litchfield said.

Click here to read about why IBM is investing \$1.5 billion in data security.

Not only were many databases unprotected by firewalls, a large percentage weren't patched. Of the SQL Server databases NGSS found, 82 percent were running SQL Server 2000. Of those, only 46 percent were running Service Pack 4, the most recent update. The rest were running SP3a or less. Four percent were completely unpatched, and vulnerable to a flaw exploited by the Slammer worm as well as an authentication flaw known as the "Hello bug."

Out of the Oracle servers, 13 percent were running versions of Oracle products for which patches are no longer issued. Such databases are known to be vulnerable to critical vulnerabilities, including flaws that can be exploited by an attacker to gain full control of a system without a user name and password.

NGSS' research also showed that people often don't deploy hotfixes. Instead, they wait for service packs. For example, out of 129 SQL Server 2000 systems NGSS found, only eight had interim fixes, and the rest were running RTM, SP3/3a or SP4.

The methodology was to probe each IP address on TCP port 1433 (SQL Server) and 1521 (Oracle). If the port was open, a version check was made, and only those systems that responded correctly to a version check were counted, in order to weed out false positives.

Some may question whether 1.160 million IP addresses is a large-enough sample from which to draw conclusions, Litchfield acknowledged. After subtracting IP ranges that are considered to be private addresses or those representing local systems, there are still a possible 3,720,183,560 addresses. Litchfield said NGSS' sample size is "accurate enough," although the 2008 sample will be larger.

To read about why Visa fined The TJX Companies' credit card processor for a massive customer data breach, click here.

NGSS last performed this survey in 2005. At that time, NGSS estimated that there were around 210,000 unprotected SQL Server databases. The growth to the 2007 estimate of 368,000 unprotected SQL Server databases is significant, but NGSS said it isn't sure whether the change is due to growth in SQL Server installs or MSDE installs—not that it would matter much were another Slammer worm to crop up.

The number of unprotected Oracle databases, by contrast, has decreased since the 2005 survey. At that time, there were some 140,000 Oracle database servers accessible on the Internet not protected by a firewall. That number has dropped to about 124,000.

Check out eWEEK.com's Security Center for the latest security news, reviews and analysis. And for insights on security coverage around the Web, take a look at [eWEEK's Security Watch blog](#).

Copyright (c) 2007 Ziff Davis Enterprise Inc. All Rights Reserved.