netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 44

November 3, 2006

Table of Contents

Product Focus

Sasser Worm Scanner – The Sasser Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Microsoft SSL Vulnerability (MS04-011) that used by the Sasser Worm to infect machines.

This Week in Review

17 individuals in phishing gang arrested. Open source and security in the enterprise. How to secure mobile IT. New ISO on security management standards.

Enjoy reading & Stay safe

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

- **Phishing gang arrested in USA and Eastern Europe after FBI investigation**

17 individuals held in investigation that covered USA, Poland and Romania
More than 20 FBI offices are said to have been involved in the investigation into the global identity theft ring, which is claimed to have been involved in a phishing attack against a major financial institution between August and October 2004.

In an investigation called "Operation Cardkeeper", FBI agents, working with local authorities, identitifed a criminal ring who were allegedly selling stolen identities, credit

card and bank account information through a forum on an internet website.

The suspected ringleader of the gang, a Polish man known as "Blindroot", is said to have hacked into third party computers to rent out webspace to other criminals who wanted to host bogus websites for the purposes of phishing.

Four arrests were made in the USA and 13 people were apprehended in Poland. The American suspects were caught with cards and machines used to encode data onto blank credit cards and when authorities attempted to search the premises, one suspect tried to flush counterfeit credit cards down the toilet. In addition to the arrests, raids were reportedly carried out in New York, Texas, Tennessee, Nebraska, Georgia and Ohio, and search warrants served on three other suspects under investigation in Romania.

Sophos

Full Story :
http://www.sophos.com/pressoffice/news/articles/2006/11/phishing-arrests.html?_log_from=rss

❖ Security on the open source road

Open source technologies are an increasingly integral element of many large-enterprise IT environments. And as such, they must be subject to the same rigorous security measures as their closed-source, commercial counterparts.

The main question facing users wishing to deploy open source in the enterprise is one of security nd the ability to patch and protect the system, identify and login users, and secure and prevent hacking attacks.

There is a general notion that open source technology components, like the Linux operating system, are more secure than commercially developed IT products.

According to Graham Titterington, principal analyst for research company Ovum, a few years ago the comparative safety of open source was "undeniably true".

He said, "The statistics on threats from both [open source and commercial] camps do not always give the big picture. But when you look at the historical frequency and severity of bugs, commercial software has been more vulnerable."
Citing an argument used by many open source proponents, he said that the more open the development process, the heavier the scrutiny it is under to discover vulnerabilities and bugs. "Any type of malware amounts to errors or vulnerabilities in the source code that hackers take advantage of. These occur mostly at the platform level in the operating system or at the database level."

However, the situation is no longer clear cut, said Titterington. For example, four years ago there were some two million lines of Linux code. Today, that has grown to more than six million, with 75,000 different functions within its kernel. The sheer scale of growth in maturity and popularity of open source challenges the effectiveness of the "many eyes" approach.

Computerweekly

Full Story :

http://www.computerweekly.com/Articles/2006/11/07/219613/Security+on+the+open+source+road.htm

❖ Keep It Secure

Tips For Securing The Mobile Enterprise
Security has long been an important mission for any IT department—serving as one of the rationales for the original formalization of the IT function in most companies—and it's generally a thankless one. Unfortunately for IT professionals, the threat environment has mushroomed since the dawn of the Internet, growing more challenging as users have become liberated from traditional office environments by the proliferation of mobile devices and services.

Today's mobile work habits raise a number of difficult problems for IT departments: How do you protect systems that are often not in the office on a controlled network? How do you protect the internal network from systems that become contaminated when on the road? What new defenses are needed for mobile systems operating on open networks? How do you protect data on portable devices even if the device itself is lost? How do you provide access to internal data and applications to roving users?

Most IT departments are still grappling with these problems, as evidenced by a survey sponsored by Symantec (www.symantec.com) at Interop last month. Although 70% of 350 respondents currently have security policies for teleworking, only 35% cannot enforce security settings on laptops and other mobile devices outside the corporate confines.

Processor

Full Story :
http://www.processor.com/editorial/article.asp?Article=articles/p2844/30p44/30p44.asp&GUID=FE70DB10483A4EEB9A1B7609847A0A07

❖ BS 7799 opens door to security work

BS 7799 has become the most widely adopted information security management standard in the world. Now known internationally as ISO 17799 and ISO/IEC 27001, the standards cover people, processes and IT systems, and help identify, quantify and manage threats to information.

The number of companies implementing ISO 27001 is increasing rapidly, and employers are seeking qualified staff, or paying for their own to be trained. There is also a demand for qualified people from security companies, and the organisations that audit and certify ISO 27001 compliance.

But working with these standards involves a management, rather than hands-on technical approach, and lacks the glamour of penetration testing. Much of the work consists of ticking boxes and making sure documents have been completed and filed correctly.

Where did it originate?

BS 7799 Part 1, written by the Department of Trade & Industry, was first published by the British Standards Institution in 1995. BS 7799 Part 2 followed in 1999.

Part 1 became ISO 17799, "Code of practice for information security management". Part 2 was adopted as ISO/IEC 27001 "Security techniques - information security management systems - requirements" in November 2005. Organisations involved in the development of the standards include the International Electrotechnical Commission (IEC), and the Organisation for Economic Co-operation and Development.

Computerweekly.com

Full Story :
http://www.computerweekly.com/Articles/2006/11/07/219616/Hot+Skills+BS+7799+opens+door+to+security+work.htm

New Vulnerabilities Tested in SecureScout

- **13456 Oracle Database Server - Oracle Spatial component Buffer Overflow Vulnerability (oct-2006/DB20)**

A Buffer overflow vulnerability exists in GEOM_OPERATION.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **Low**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html

Other references:
http://www.databasesecurity.com/oracle/OracleOct2006-CPU-Analysis.pdf
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2006-5344

- **13457 Oracle Database Server - Oracle Spatial component SQL Injection Vulnerability (oct-2006/DB21)**

An SQL Injection and buffer overflow vulnerability exists in TRANSFORM_LAYER.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **Low**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html

Other references:
http://www.databasesecurity.com/oracle/OracleOct2006-CPU-Analysis.pdf

http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2006-5344

❖ 13458 Oracle Database Server - Oracle Spatial component Length Check Vulnerability (oct-2006/DB22)

A Length checking vulnerability exists in RELATE function – then calls MD2.RELATE (see DB03 and DB11). As MDSYS is not in the exclusion list for Oracle Application Server this flaw could be exploited without a user ID and password via the PLSQL Gateway.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **Low**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html

Other references:
http://www.databasesecurity.com/oracle/OracleOct2006-CPU-Analysis.pdf
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2006-5345

❖ 13459 Oracle Database Server - Dictionary component unspecified Vulnerability (Alert 68/aug-04/DB01)

An unspecified vulnerability exists in Oracle Database Server Dictionary component.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **Medium**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf

Other references:
iDEFENSE:
http://www.idefense.com/application/poi/display?id=135&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=136&type=vulnerabilities

Red Database Security:

http://www.red-database-security.com/advisory/advisory_20040903_1.html
http://www.red-database-security.com/advisory/advisory_20040903_2.html
http://www.red-database-security.com/advisory/advisory_20040903_3.html

Application Security:
http://www.appsecinc.com/resources/alerts/oracle/2004-0001/

Integrigy:
http://www.integrigy.com/alerts/OraAlert68OraAppsImpact.htm

Pentest Limited:
http://www.pentest.co.uk/documents/ptl-2004-04.html

US-CERT VU#170830:
http://www.kb.cert.org/vuls/id/170830

US-CERT VU#435974:
http://www.kb.cert.org/vuls/id/435974

US-CERT VU#316206:
http://www.kb.cert.org/vuls/id/316206

BID:11099
http://www.securityfocus.com/bid/11099

BID:11100
http://www.securityfocus.com/bid/11100

BID:10871
http://www.securityfocus.com/bid/10871

Secunia:
http://secunia.com/advisories/12409/

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2004-0637
CAN-2004-0638
CAN-2004-1338
CAN-2004-1339
CAN-2004-1362
CAN-2004-1363
CAN-2004-1364
CAN-2004-1366
CAN-2004-1367
CAN-2004-1368
CAN-2004-1369
CAN-2004-1370

CAN-2004-1371

❖ 13460 Oracle Database Server - Extproc component unspecified Vulnerability (Alert 68/aug-04/DB02)

An unspecified vulnerability exists in Oracle Database Server Extproc component.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **Medium**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf

Other references:
iDEFENSE:
http://www.idefense.com/application/poi/display?id=135&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=136&type=vulnerabilities

Red Database Security:
http://www.red-database-security.com/advisory/advisory_20040903_1.html
http://www.red-database-security.com/advisory/advisory_20040903_2.html
http://www.red-database-security.com/advisory/advisory_20040903_3.html

Application Security:
http://www.appsecinc.com/resources/alerts/oracle/2004-0001/

Integrigy:
http://www.integrigy.com/alerts/OraAlert68OraAppsImpact.htm

Pentest Limited:
http://www.pentest.co.uk/documents/ptl-2004-04.html

US-CERT VU#170830:
http://www.kb.cert.org/vuls/id/170830

US-CERT VU#435974:
http://www.kb.cert.org/vuls/id/435974

US-CERT VU#316206:
http://www.kb.cert.org/vuls/id/316206

BID:11099
http://www.securityfocus.com/bid/11099

BID:11100
http://www.securityfocus.com/bid/11100

BID:10871
http://www.securityfocus.com/bid/10871

Secunia:
http://secunia.com/advisories/12409/

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2004-0637
CAN-2004-0638
CAN-2004-1338
CAN-2004-1339
CAN-2004-1362
CAN-2004-1363
CAN-2004-1364
CAN-2004-1366
CAN-2004-1367
CAN-2004-1368
CAN-2004-1369
CAN-2004-1370

CAN-2004-1371

❖ 13461 Oracle Database Server - Core SQL component unspecified Vulnerability (Alert 68/aug-04/DB03)

An unspecified vulnerability exists in Oracle Database Server Core SQL component.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **Medium**

References:

References:
Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf

Other references:
iDEFENSE:
http://www.idefense.com/application/poi/display?id=135&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=136&type=vulnerabilities

Red Database Security:
http://www.red-database-security.com/advisory/advisory_20040903_1.html
http://www.red-database-security.com/advisory/advisory_20040903_2.html
http://www.red-database-security.com/advisory/advisory_20040903_3.html

Application Security:
http://www.appsecinc.com/resources/alerts/oracle/2004-0001/

Integrigy:
http://www.integrigy.com/alerts/OraAlert68OraAppsImpact.htm

Pentest Limited:
http://www.pentest.co.uk/documents/ptl-2004-04.html

US-CERT VU#170830:
http://www.kb.cert.org/vuls/id/170830

US-CERT VU#435974:
http://www.kb.cert.org/vuls/id/435974

US-CERT VU#316206:
http://www.kb.cert.org/vuls/id/316206

BID:11099
http://www.securityfocus.com/bid/11099

BID:11100
http://www.securityfocus.com/bid/11100

BID:10871
http://www.securityfocus.com/bid/10871

Secunia:
http://secunia.com/advisories/12409/

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2004-0637
CAN-2004-0638
CAN-2004-1338
CAN-2004-1339
CAN-2004-1362
CAN-2004-1363
CAN-2004-1364
CAN-2004-1366
CAN-2004-1367
CAN-2004-1368
CAN-2004-1369
CAN-2004-1370

CAN-2004-1371

❖ **13462 Oracle Database Server - Oracle Text component unspecified Vulnerability (Alert 68/aug-04/DB04)**

An unspecified vulnerability exists in Oracle Database Server Oracle Text component.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **Medium**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf

Other references:
iDEFENSE:
http://www.idefense.com/application/poi/display?id=135&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=136&type=vulnerabilities

Red Database Security:
http://www.red-database-security.com/advisory/advisory_20040903_1.html
http://www.red-database-security.com/advisory/advisory_20040903_2.html
http://www.red-database-security.com/advisory/advisory_20040903_3.html

Application Security:
http://www.appsecinc.com/resources/alerts/oracle/2004-0001/

Integrigy:
http://www.integrigy.com/alerts/OraAlert68OraAppsImpact.htm

Pentest Limited:
http://www.pentest.co.uk/documents/ptl-2004-04.html

US-CERT VU#170830:
http://www.kb.cert.org/vuls/id/170830

US-CERT VU#435974:
http://www.kb.cert.org/vuls/id/435974

US-CERT VU#316206:
http://www.kb.cert.org/vuls/id/316206

BID:11099
http://www.securityfocus.com/bid/11099

BID:11100
http://www.securityfocus.com/bid/11100

BID:10871
http://www.securityfocus.com/bid/10871

Secunia:
http://secunia.com/advisories/12409/

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2004-0637
CAN-2004-0638
CAN-2004-1338
CAN-2004-1339
CAN-2004-1362
CAN-2004-1363
CAN-2004-1364
CAN-2004-1366
CAN-2004-1367
CAN-2004-1368
CAN-2004-1369
CAN-2004-1370

CAN-2004-1371

❖ **13463 Oracle Database Server - DDL component unspecified Vulnerability (Alert 68/aug-04/DB05)**

An unspecified vulnerability exists in Oracle Database Server DDL component.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **Medium**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf

Other references:
iDEFENSE:
http://www.idefense.com/application/poi/display?id=135&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=136&type=vulnerabilities

Red Database Security:
http://www.red-database-security.com/advisory/advisory_20040903_1.html
http://www.red-database-security.com/advisory/advisory_20040903_2.html
http://www.red-database-security.com/advisory/advisory_20040903_3.html

Application Security:
http://www.appsecinc.com/resources/alerts/oracle/2004-0001/

Integrigy:
http://www.integrigy.com/alerts/OraAlert68OraAppsImpact.htm

Pentest Limited:
http://www.pentest.co.uk/documents/ptl-2004-04.html

US-CERT VU#170830:
http://www.kb.cert.org/vuls/id/170830

US-CERT VU#435974:
http://www.kb.cert.org/vuls/id/435974

US-CERT VU#316206:
http://www.kb.cert.org/vuls/id/316206

BID:11099
http://www.securityfocus.com/bid/11099

BID:11100
http://www.securityfocus.com/bid/11100

BID:10871
http://www.securityfocus.com/bid/10871

Secunia:
http://secunia.com/advisories/12409/

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2004-0637
CAN-2004-0638
CAN-2004-1338
CAN-2004-1339
CAN-2004-1362
CAN-2004-1363
CAN-2004-1364
CAN-2004-1366
CAN-2004-1367
CAN-2004-1368
CAN-2004-1369
CAN-2004-1370

CAN-2004-1371

❖ **13464 Oracle Database Server - Core SQL component unspecified Vulnerability (Alert 68/aug-04/DB06)**

An unspecified vulnerability exists in Oracle Database Server Core SQL component.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Gather Info** Risk: **Medium**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf

Other references:
iDEFENSE:
http://www.idefense.com/application/poi/display?id=135&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=136&type=vulnerabilities

Red Database Security:
http://www.red-database-security.com/advisory/advisory_20040903_1.html
http://www.red-database-security.com/advisory/advisory_20040903_2.html
http://www.red-database-security.com/advisory/advisory_20040903_3.html

Application Security:
http://www.appsecinc.com/resources/alerts/oracle/2004-0001/

Integrigy:
http://www.integrigy.com/alerts/OraAlert68OraAppsImpact.htm

Pentest Limited:
http://www.pentest.co.uk/documents/ptl-2004-04.html

US-CERT VU#170830:
http://www.kb.cert.org/vuls/id/170830

US-CERT VU#435974:
http://www.kb.cert.org/vuls/id/435974

US-CERT VU#316206:
http://www.kb.cert.org/vuls/id/316206

BID:11099
http://www.securityfocus.com/bid/11099

BID:11100
http://www.securityfocus.com/bid/11100

BID:10871
http://www.securityfocus.com/bid/10871

Secunia:
http://secunia.com/advisories/12409/

Product Homepage:
http://www.oracle.com

CVE Reference: CVE-2004-0637
CAN-2004-0638
CAN-2004-1338
CAN-2004-1339
CAN-2004-1362
CAN-2004-1363
CAN-2004-1364
CAN-2004-1366
CAN-2004-1367
CAN-2004-1368
CAN-2004-1369
CAN-2004-1370

CAN-2004-1371

❖ **13465 Oracle Database Server - Core SQL component unspecified Vulnerability (Alert 68/aug-04/DB07)**

An unspecified vulnerability exists in Oracle Database Server Core SQL component.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Gather Info** Risk: **Medium**

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf

Other references:
iDEFENSE:
http://www.idefense.com/application/poi/display?id=135&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=136&type=vulnerabilities

Red Database Security:
http://www.red-database-security.com/advisory/advisory_20040903_1.html
http://www.red-database-security.com/advisory/advisory_20040903_2.html
http://www.red-database-security.com/advisory/advisory_20040903_3.html

Application Security:
http://www.appsecinc.com/resources/alerts/oracle/2004-0001/

Integrigy:
http://www.integrigy.com/alerts/OraAlert68OraAppsImpact.htm

Pentest Limited:
http://www.pentest.co.uk/documents/ptl-2004-04.html

US-CERT VU#170830:
http://www.kb.cert.org/vuls/id/170830

US-CERT VU#435974:
http://www.kb.cert.org/vuls/id/435974

US-CERT VU#316206:
http://www.kb.cert.org/vuls/id/316206

BID:11099
http://www.securityfocus.com/bid/11099

BID:11100
http://www.securityfocus.com/bid/11100

BID:10871
http://www.securityfocus.com/bid/10871

Secunia:
http://secunia.com/advisories/12409/

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2004-0637
CAN-2004-0638
CAN-2004-1338
CAN-2004-1339
CAN-2004-1362
CAN-2004-1363
CAN-2004-1364
CAN-2004-1366
CAN-2004-1367
CAN-2004-1368
CAN-2004-1369
CAN-2004-1370

CAN-2004-1371

New Vulnerabilities found this Week

Microsoft Visual Studio WMI Object Broker ActiveX Control Code Execution

"Execution of arbitrary code"

A vulnerability has been reported in Microsoft Visual Studio, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an unspecified error in the WMI Object Broker ActiveX Control (WmiScriptUtils.dll).

Successful exploitation allows execution of arbitrary code when a user e.g. visits a malicious website using Internet Explorer.

The vulnerability is reported in Microsoft Visual Studio 2005.

NOTE: The vulnerability is already being actively exploited.

References:
http://www.microsoft.com/technet/security/advisory/927709.mspx

Microsoft Windows Internet Connection Sharing Denial of Service

"Denial of Service"

h07 has discovered a vulnerability in Microsoft Windows, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to a NULL pointer dereference error in Windows NAT Helper Components (ipnathlp.dll). This can be exploited to crash the service via a specially crafted DNS query.

Successful exploitation requires that Internet Connection Sharing is enabled and the query is received from a client on the shared network interface.

The vulnerability is confirmed in a fully patched Windows XP SP2 system. Other versions may also be affected.

References:
http://milw0rm.com/exploits/2672

Apple Xcode GDB "DWARF" Buffer Overflow

"Gain escalated privileges"

Apple has acknowledged a vulnerability in GDB included in Xcode, which potentially can be exploited by malicious, local users to gain escalated privileges or malicious people to compromise a vulnerable system.

References:
http://docs.info.apple.com/article.html?artnum=304669

Sun ONE/Java System Web Server NSS Denial of Service
"Denial of Service"

A vulnerability has been reported in Sun ONE Application Server and Sun Java System Web Server, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error in Network Security Services (NSS), which can be exploited to cause the server to exit.

Note: The vulnerability affects only systems, which have SSLv2 enabled.

The vulnerability is reported in Sun Java System Web Server 6.0 and Sun ONE Application Server 7.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102670-1

Internet Explorer 7 Window Injection Vulnerability
"Spoof the content of a pop-up window"

A vulnerability has been discovered in Internet Explorer 7, which can be exploited by malicious people to spoof the content of websites.

The problem is that a website can inject content into another site's window if the target name of the window is known. This can e.g. be exploited by a malicious website to spoof the content of a pop-up window opened on a trusted website.

The vulnerability has been confirmed on a fully patched system with Internet Explorer 7.0 and Microsoft Windows XP SP2.

References:
http://secunia.com/advisories/22628/

Cisco Security Agent for Linux Port Scan Denial of Service
"Denial of Service"

A vulnerability has been reported in Cisco Security Agent for Linux, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error within the detection of port scans. This can be exploited to stop the Cisco Security Agent (CSA) from responding due to excessive resource consumption by starting a port scan with certain options.

The vulnerability is reported in CSA 4.5 for Linux prior to Hotfix 4.5.1.657, CSA 5.0 for Linux prior to Hotfix 5.0.0.193, and in the standalone CSA shipped with Cisco Unified CallManager (CUCM) 5.0 versions including 5.0(4), and Cisco Unified Presence Server (CUPS) 1.0 versions including 1.0(2).

References:
http://www.cisco.com/en/US/products/products_security_advisory09186a00807693c7.shtml

Vulnerability Resource
Check out this compendium of links and up-to-the minute information about network security issues. Their claim to be the 'security portal for information system security professionals' is well founded. http://www.infosyssec.org/infosyssec/

Thank You
Thanks for sifting through another great edition of the ScoutNews. We hope we captured a flavor for the week and gave you just enough information on newly found vulnerabilities to keep you up-to-date. To subscribe or unsubscribe, contact us at ScoutNews@netVigilance.com.

About SecureScout
SecureScout is a leading vulnerability scanner and management tool developed and marketed worldwide by NexantiS Corporation.
SecureScout is a trademark of NexantiS Corporation.
netVigilance, Inc. is a partner of NexantiS and an authorized distributor of SecureScout.

For any inquiry about SecureScout by:
Customers in America and Northern Europe contact us at info@netVigilance.com
Customers in France, Italy, Spain, Portugal, Greece, Turkey, Eastern Europe, Middle East, Africa and Asia/Pacific, contact NexantiS at info-scanner@securescout.net