netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 45

November 10, 2006

Table of Contents

Product Focus

Spida Digispid Worm Scanner – The Spida Digispid Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are prone any of the Microsoft Java Virtual Machine Vulnerabilities (MS02-069).

This Week in Review

How to survive a security breach. Services helping softwareproducers make secure products. VoIP – use the safegueards already there. McAfee's and other's fears not without reason.

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

- **Surviving a Security Breach: Assume the worst will happen and plan for it**

When analysing threats to an organisation we need to calculate the risk each threat poses. Risk is comprised of two elements – probability and impact.

The negative impacts which would result from a threat materialising can be determined fairly accurately through a process such as the business impact analysis, or BIA, generally employed as part of a business continuity management programme. Negative impacts

such as loss of revenue, lost business opportunity, breach of legislation and/or regulation, customer dissatisfaction, negative brand impact, loss of market share etc. can be explored with relevant business representatives to arrive at a likely cost to the organisation should the threat materialise.

Based on the risk score the organisation then usually agrees the course of action to manage the threat i.e. to accept, transfer, treat or avoid the risk. The problem is that the scoring of probability is inherently flawed.

How high would you rate the probability of your home being broken into? You may say that the probability is "very low" given your low crime neighbourhood, security locks, burglar alarm and history of no burglaries in your street in the last ten years.

Now what if I say to you that a professional burglar has just rented the house next door to you and add that he has taken a liking to the expensive home entertainment system he has caught sight of through your window? I would guess that the probability rating has just moved up a notch or two.

Securitypark.net

Full Story :
http://www.securitypark.co.uk/article.asp?articleid=26098&CategoryID=1

- **Application security bolstered by new services**

Ten years into Web applications and organizations are still wrestling with security issues, said Jeff Williams, CEO and cofounder of Aspect Security Inc., and chair of the OWASP Foundation. "Every application we look at has dozens of flaws, and certainly some critical ones, and those are the folks who've self-selected for a security review," he said.
Now throw in new technology like Ajax and Web services, and organizations are barely scratching the surface of understanding the accompanying security issues, he said.
"That's a recipe for introducing serious security flaws," according to Williams.

At the heart of the matter has been the lack of a programmatic, repeatable approach to building security into the software development life cycle, according to Stephen A. Barlock, North America Security Practice Lead for Accenture. Now organizations such as Accenture, in a recently announced partnership with Symantec, and Aspect Security are launching services to help address this need.

Computerweekly

Full Story :
http://www.computerweekly.com/Articles/2006/11/09/219845/Application+security+bolstered+by+new+services.htm

- **VoIP security safeguards -- they may be there already**

Wanna be clued in on a little secret? VoIP security isn't all that difficult after all.

Actually, a lot of the necessary tools and tricks to lock down and secure a voice network are there already, they just have to be used correctly.

"It's not an add-on," Kevin Flynn, senior manager of unified communications for Cisco, said about VoIP security "It's built into the network already or in the VoIP products themselves."

According to Flynn, pretty much every facet of VoIP security should already be part of the data network, so finding ways to apply them to VoIP should be a breeze.

"These are things a company ought to be doing anyway," he said. "They ought to be doing antivirus in the network, access control and IDS. It's stuff they already own."

Yankee Group vice president Zeus Kerravala agreed. He said some of the biggest security issues affecting VoIP now are not necessarily VoIP specific, but broader networking issues. He said many more voice-specific concerns stem from vendor hype than from actual issues.

"You can take care of a lot of [VoIP security issues] with QoS and by minimizing the amount of malicious traffic on the network," Kerravala said. "But you should be doing that already anyway."

Computerweekly

Full Story :
http://www.computerweekly.com/Articles/2006/11/09/219844/VoIP+security+safeguards+--+they+may+be+there+already.htm

❖ Microsoft's Allchin: Vista won't need antivirus

Microsoft co-president Jim Allchin has suggested that some Vista users will not need to run any third-party antivirus software.

Allchin made the comments in a telephone conference with reporters on Wednesday, according to betanews.com. He said that while there was no way of knowing that security perfection had been achieved in Vista, he was confident enough in the operating system to let his seven-year-old use a locked down version without antivirus.

"My son, seven years old, runs Windows Vista and, honestly, he doesn't have an antivirus system on his machine. His machine is locked down with parental controls, he can't download things unless it's to the places that I've said that he could do, and I'm feeling totally confident about that," said Allchin. "That is quite a statement. I couldn't say that in Windows XP SP2."

Allchin said his confidence in Vista came from new security features, including parental controls and Address Space Layout Randomisation, which is a feature that randomises key data areas in the virtual computer space in an effort to foil hacks based on predictable data storage.

ZDNet

Full Story :

http://news.zdnet.co.uk/security/0,1000000189,39284664,00.htm

New Vulnerabilities Tested in SecureScout

- **13466 Oracle Database Server - Core SQL component unspecified Vulnerability (Alert 68/aug-04/DB08)**

An unspecified vulnerability exists in Oracle Database Server Core SQL 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: 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

❖ 13467 Oracle Database Server - Export component unspecified Vulnerability (Alert 68/aug-04/DB09)

An unspecified vulnerability exists in Oracle Database Server Export component.

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

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: 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

❖ 13468 An unspecified vulnerability exists in Oracle Database Server Oracle Spatial component.

The vulnerability can be exploited to cause a DoS (Denial of Service), or conduct SQL injection attacks.

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

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: 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

❖ **13469 Oracle Database Server - Oracle Spatial component unspecified Vulnerability (Alert 68/aug-04/DB11)**

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

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

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

❖ 13470 Oracle Database Server - Listener component unspecified Vulnerability (Alert 68/aug-04/DB12)

An unspecified vulnerability exists in Oracle Database Server Listener component.

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

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

❖ **13471 An unspecified vulnerability exists in Oracle Database Server XDB component.**

Oracle Database Server - XDB component unspecified Vulnerability (Alert 68/aug-04/DB13)

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

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

❖ **13472 Oracle Database Server - DBCA component unspecified Vulnerability (Alert 68/aug-04/DB14)**

An unspecified vulnerability exists in Oracle Database Server DBCA component.

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

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

❖ **13473 Oracle Database Server - Oracle Text component unspecified Vulnerability (Alert 68/aug-04/DB15)**

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

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

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

❖ 13474 Oracle Database Server - Oracle Spatial component unspecified Vulnerability (Alert 68/aug-04/DB16)

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

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

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

❖ **17936 DigiOz Guestbook Path Disclosure Vulnerability**

The DigiOz Guestbook is a PHP driven guestbook system.
A vulnerability exists in list.php script which allows remote attackers to obtain sensitive information via an HTTP request to list.php that contains wrong value in page parameter.

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

References:

Original Advisory:
http://netvigilance.com/advisory0006

Other references:
* FULLDISC:20061107 DigiOz Guestbook version 1.7 Path Disclosure
* URL:http://marc.theaimsgroup.com/?l=full-disclosure&m=116288079420333&w=2
* BUGTRAQ:20061107 DigiOz Guestbook version 1.7 Path Disclosure
* URL:http://www.securityfocus.com/archive/1/450826/30/0/threaded
* OSVDB:29985
* URL:http://www.osvdb.org/29985

Product Home-Page:
http://www.digioz.com/phpscripts.php

CVE Reference: CVE-2006-5651

New Vulnerabilities found this Week

Mozilla Firefox and SeaMonkey Multiple Vulnerabilities

"Bypass certain security restrictions; conduct cross-site scripting attacks"

Some vulnerabilities have been reported in Mozilla Firefox and Mozilla SeaMonkey, which can be exploited by malicious people to bypass certain security restrictions, conduct cross-site scripting attacks, and potentially compromise a vulnerable system.

1) The bundled Network Security Services (NSS) library contains an incomplete fix for the RSA signature verification vulnerability reported in MFSA 2006-60.

2) An error exists within the handling of Script objects. This can potentially be exploited to execute arbitrary JavaScript bytecode by modifying already running Script objects.

3) Some unspecified errors in the layout engine and memory corruption errors in the JavaScript engine can be exploited to crash the application and may allow execution of arbitrary code.

4) An unspecified error within XML.prototype.hasOwnProperty can potentially be

exploited to execute arbitrary code.

References:
http://www.mozilla.org/security/announce/2006/mfsa2006-65.html
http://www.mozilla.org/security/announce/2006/mfsa2006-66.html
http://www.mozilla.org/security/announce/2006/mfsa2006-67.html
http://www.kb.cert.org/vuls/id/815432
http://www.kb.cert.org/vuls/id/495288
http://www.kb.cert.org/vuls/id/335392
http://www.kb.cert.org/vuls/id/714496

Microsoft XMLHTTP ActiveX Control Code Execution Vulnerability

"Execution of arbitrary code"

A vulnerability has been discovered in Microsoft XML Core Services, which can be exploited by malicious people to compromise a users system.

The vulnerability is caused due to an error in the XMLHTTP 4.0 ActiveX Control (msxml4.dll) within the "setRequestHeader()" method.

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

The vulnerability is confirmed on a fully patched Windows XP SP2 system with msxml4.dll version 4.20.9818.0 installed.

NOTE: The vulnerability is already being actively exploited.

References:
http://www.microsoft.com/technet/security/advisory/927892.mspx
http://www.kb.cert.org/vuls/id/585137

OpenSSH Privilege Separation Monitor Weakness

"Bypass certain security restrictions**"**

A weakness has been reported in OpenSSH, which can be exploited by malicious people to bypass certain security restrictions.

The weakness is caused due to an error within the privilege separation monitor, which may weaken the authentication process.

Reportedly, the weakness can only be exploited in combination with other vulnerabilities.

The weakness is reported in version 4.4. Other versions may also be affected.

References:
http://www.openssh.org/txt/release-4.5

Linux Kernel Fragmented IPv6 Packet Filtering Bypass

"Bypass filtering rules"

Some vulnerabilities have been reported in the Linux Kernel, which can be exploited by

malicious people to bypass certain security restrictions.

The vulnerabilities are caused due to the incorrect processing of certain fragmented IPv6 packets. This can be exploited to bypass filtering rules by sending specially crafted packets.

References:
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=51d8b1a65291a6956b79374b6adbbadc2263bcf6
http://www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=6d381634d213580d40d431e7664dfb45f641b884

ICQ ICQPhone.SipxPhoneManager ActiveX Control Vulnerability

"Download and execute an arbitrary file; execution of arbitrary code"

A vulnerability has been reported in America Online ICQ, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a design error in the ICQPhone.SipxPhoneManager ActiveX control within the "DownloadAgent()" method. This can be exploited to download and execute an arbitrary file on a user's system by e.g. using a malicious ICQ avatar to message the user.

Successful exploitation allows execution of arbitrary code.

The vulnerability is reported in version 5.1. Other versions may also be affected.

References:
http://www.zerodayinitiative.com/advisories/ZDI-06-037.html

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