netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 3

January 18, 2008

Table of Contents

Product Focus

Messenger Service Vulnerability Scanner – The Messenger Service Vulnerability 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 Windows Messenger Service flaw (MS03-043).

Check out our video section for a number of interviews with Jesper Jurcenoks:
www.netvigilance.com/videos

This Week in Review

A warning from the security experts. TJX - a year after.New web-site to help e-crime victims. The 'greynets' on your network.

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

- **Malware writers gear up for bumper 2008**

Security experts have warned users to focus on securing their whole online lifestyle in 2008.

Care should be taken in all aspects of online services, including bill payments,

shopping and stock trading, and not just in the use of social networking and gaming sites.

"Social engineering will still be the preferred method to lure people into infecting their computer or giving away password information, but the approaches will become much more sophisticated," said Diego d'Ambra, chief technology officer at SoftScan.

vnunet

Full Story :
http://www.vnunet.com/vnunet/news/2207573/tips-staying-safe-2008

❖ One year later: Five takeaways from the TJX breach

The retailer has survived the massive data theft, but the card industry remains unsettled One year ago today, The TJX Companies Inc. disclosed what has turned out to be the largest information security breach involving credit and debit card data -- thus far, at least.

The data compromise at the Framingham, Mass.-based retailer began in mid-2005, with system intrusions at two Marshalls stores in Miami via poorly protected wireless LANs. The intruders who broke into TJX's payment systems remained undetected for 18 months, during which time they downloaded a total of 80GB of cardholder data.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9057758&taxonomyId=17&intsrc=kc_top

❖ Support for e-crime victims

The first web site dedicated to helping victims of e-crime has been set up.

The www.e-victims.org will feed information to trading standards, the Office of Fair Trading and police where necessary.

The site will help tackle the growing threat of electronic crime, said Lord Erroll, a member of the House of Lords committee on personal internet security.

"Online scams today are getting more sophisticated and they will catch more people out - that is why we need the service to support internet users," he said.

The site will provide advice to victims as well as recording independent statistics.

vnunet

Full Story :
http://www.vnunet.com/computing/news/2207550/web-site-support-crime-victims

- **What is a greynet?**

Internet communications have evolved from point-to-point, asynchronous channels like email to real-time, presence-oriented communications like IM, P2P file sharing, Skype, and web conferencing. FaceTime terms these real-time communications applications 'greynets' – defined as network-enabled applications that are often downloaded and installed by the end user without the permission or knowledge of the IT department and that use evasive techniques to circumvent existing security controls.

Help net security

Full Story :
http://www.net-security.org/secworld.php?id=5733

New Vulnerabilities Tested in SecureScout

- **16831 Oracle Application Server - Oracle Forms component unspecified Vulnerability (jan-2008/AS04)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Forms component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html

CVE Reference:

- **16830 Oracle Application Server - Oracle BPEL Worklist Application component unspecified Vulnerability (jan-2008/AS03)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle BPEL Worklist Application component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html

CVE Reference:

❖ **13618 Oracle Database Server - Core RDBMS component unspecified Vulnerability (jan-2008/DB08)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server Core RDBMS component.

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

References:

* CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html

CVE Reference:

❖ **13617 Oracle Database Server - Oracle Spatial component unspecified Vulnerability (jan-2008/DB07)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server Oracle Spatial component.

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

References:

* CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html

CVE Reference:

❖ **13616 Oracle Database Server - Oracle Spatial component unspecified Vulnerability (jan-2008/DB06)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server Oracle Spatial component.

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

References:

* CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html

CVE Reference:

❖ 13615 Oracle Database Server - Upgrade/Downgrade component unspecified Vulnerability (jan-2008/DB05)

An unspecified vulnerability with unknown impact exists in Oracle Database Server Upgrade/Downgrade component.

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

References:

* CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html

CVE Reference:

❖ 13614 Oracle Database Server - Oracle Spatial component unspecified Vulnerability (jan-2008/DB04)

An unspecified vulnerability with unknown impact exists in Oracle Database Server Oracle Spatial component.

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

References:

* CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html

CVE Reference:

❖ 13613 Oracle Database Server - Advanced Queuing component unspecified Vulnerability (jan-2008/DB03)

An unspecified vulnerability with unknown impact exists in Oracle Database Server Advanced Queuing component.

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

References:

* CONFIRM: http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html

CVE Reference:

❖ **13612 Oracle Database Server - Advanced Queuing component unspecified Vulnerability (jan-2008/DB02)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server Advanced Queuing component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html

CVE Reference:

❖ **13611 Oracle Database Server - XML DB component unspecified Vulnerability (jan-2008/DB01)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server XML DB component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html

CVE Reference:

New Vulnerabilities found this Week

Cisco Unified Communications Manager CTL Provider Service Buffer Overflow
"Denial of Service"

Cody Pierce has reported a vulnerability in Cisco Unified Communications Manager (CUCM), which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the CTL Provider Service (CTLProvider.exe) and can be exploited to cause a heap-based buffer overflow via a specially crafted packet sent to default port 2444/TCP.

Successful exploitation allows execution of arbitrary code.

The vulnerability affects the following versions:

* Cisco Unified CallManager 4.0
* Cisco Unified CallManager 4.1 versions prior to 4.1(3)SR5c
* Cisco Unified Communications Manager 4.2 versions prior to 4.2(3)SR3
* Cisco Unified Communications Manager 4.3 versions prior to 4.3(1)SR1

References:
http://dvlabs.tippingpoint.com/advisory/TPTI-08-02

Microsoft Excel File Handling Code Execution

"execution of arbitrary code"

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

The vulnerability is caused due to an unspecified error in the handling of Excel files and can be exploited via a specially crafted Excel file with malformed header information.

Successful exploitation allows execution of arbitrary code but requires that the user is tricked into opening a malicious Excel file.

NOTE: According to Microsoft, this is currently being actively exploited.

The vulnerability is reported in the following versions:
* Microsoft Office Excel 2003 Service Pack 2
* Microsoft Office Excel Viewer 2003
* Microsoft Office Excel 2002
* Microsoft Office Excel 2000
* Microsoft Excel 2004 for Mac.

References:
http://www.microsoft.com/technet/security/advisory/947563.mspx

Cisco VPN Client IPSec Driver Local Denial of Service

"Denial of Service"

mu-b has reported a vulnerability in Cisco VPN Client, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

The vulnerability is caused due to an error when handling certain IOCTLs sent to the IPSec driver (CVPNDRVA.sys). This can be exploited to cause a memory corruption within kernel space by sending specially crafted IOCTLs to the affected driver, resulting in a system crash.

The vulnerability is reported in CVPNDRVA.sys version 5.0.02.0090. Other versions may also be affected.

References:
http://milw0rm.com/exploits/4911

Oracle Products Multiple Vulnerabilities

Multiple vulnerabilities with unknown impacts have been reported for various Oracle products, which can be exploited by malicious users and malicious people.

The vulnerabilities are caused due to unspecified errors. No more information is currently available.

The vulnerabilities are reported in the following products and versions:
• Oracle Database 11g, version 11.1.0.6
• Oracle Database 10g Release 2, versions 10.2.0.2, 10.2.0.3
• Oracle Database 10g, version 10.1.0.5
• Oracle Database 9i Release 2, versions 9.2.0.8, 9.2.0.8DV
• Oracle Application Server 10g Release 3 (10.1.3), versions 10.1.3.0.0, 10.1.3.1.0, 10.1.3.3.0
• Oracle Application Server 10g Release 2 (10.1.2), versions 10.1.2.0.2, 10.1.2.1.0, 10.1.2.2.0
• Oracle Application Server 10g (9.0.4), version 9.0.4.3
• Oracle Collaboration Suite 10g, version 10.1.2
• Oracle E-Business Suite Release 12, versions 12.0.0 - 12.0.3
• Oracle E-Business Suite Release 11i, versions 11.5.9 - 11.5.10 CU2
• Oracle PeopleSoft Enterprise PeopleTools versions 8.22, 8.48, 8.49

References:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html

Apple QuickTime Multiple Vulnerabilities
"execution of arbitrary code"

Some vulnerabilities have been reported in Apple QuickTime, which can be exploited by malicious people to compromise a vulnerable system.

1) An unspecified error exists in the handling of Sorenson 3 video files, which can be exploited to cause a memory corruption and may allow execution of arbitrary code.

2) An error exists in the processing of Macintosh Resources embedded in QuickTime movies. This can be exploited to cause a memory corruption via an overly large length value stored in the resource header in a specially crafted QuickTime movie file.

3) An error in the parsing of malformed Image Descriptor (IDSC) atoms can be exploited to cause a heap corruption via a specially crafted movie file.

4) A boundary error exists within the processing of compressed PICT images and can be exploited to cause a buffer overflow.

Successful exploitation of these vulnerabilities may allow execution of arbitrary code.

References:
http://docs.info.apple.com/article.html?artnum=307301

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