netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 2

January 11, 2008

Table of Contents

Product Focus

CodeRed Worm Scanner – The CodeRed Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any have been infected by CodeRed Worm.

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

This Week in Review

Stronger regulations on internet advertising on the way. Software companies use actual customer data for testing purposes. Security enthusiast figures out how to spam your printer. A comprehensive threat defense guide.

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

- **FTC issues ad-tracking guidelines**

US consumer protection body the Federal Trade Commission has backed a tightening of rules on internet advertising and the use of personal information. It has proposed stronger industry regulation of the tracking of users' habits.

Online advertising is often based on information about a user's browsing habits, but the FTC said consumers are often unaware of this and are not given a chance to object. It has proposed a set of principles that it says should be adopted by industry.

The Register

Full Story :
http://www.theregister.co.uk/2008/01/10/ftc_ad_track_guidelines/

❖ Software developers putting data at risk

Over half of UK companies use actual rather than disguised customer data to test applications during the development process, according to a survey by Compuware Corporation.

The report, created in conjunction with privacy management firm the Ponemon Institute, concludes that this practice compromises critical information as these environments are less secure than production environments.

Testing data may be exposed to a variety of unauthorised sources, including in-house staff, consultants, partners and even offshore personnel.

vnunet

Full Story :
http://www.vnunet.com/vnunet/news/2206925/software-developers-data-risk

❖ Printers vulnerable to spamming attacks

A US-based security enthusiast has figured out how to send spam to a person's printer from an infected Web page.
Aaron Weaver made the discovery that the world could probably do without, by using a little-known capability found in most Web browsers. Using this, Weaver can make a Web page launch a print job on just about any printer on a victim's network. The website could print annoying ads on the printer and theoretically issue more dangerous commands, like telling the printer to send a fax, format its hard drive or download new firmware.

techworld

Full Story :
http://www.techworld.com/security/news/index.cfm?newsID=11090&pagtype=samechan

❖ Adaptive Threat Defense Demo: Building a Secure Network

The presenter of this webcast demonstrates how customers can more effectively manage and multigate risks posed to their networked business systems and application.

Understanding Architecture: John Chambers at RSA 2005 - Part 3

At the RSA conference the presenter of this webcast talks about self-defending networks, multiple layers of defense for a network and security in healthcare.

zdnet

Full Story :
http://whitepapers.zdnet.co.uk/0,1000000651,260292736p-39000361q,00.htm

New Vulnerabilities Tested in SecureScout

- **16825 LSASS Bypass Vulnerability (MS08-002/943485) (Remote File Checking)**

An elevation of privilege vulnerability exists in the Microsoft Windows Local Security Authority Subsystem Service (LSASS) due to its improper handling of local procedure call (LPC) requests. The vulnerability could allow an attacker to run code with elevated privileges. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

* MS: MS08-002
http://www.microsoft.com/technet/security/Bulletin/MS08-002.mspx
* CERT: TA08-008A
http://www.us-cert.gov/cas/techalerts/TA08-008A.html
* SECUNIA: 28341
http://secunia.com/advisories/28341

CVE Reference: CVE-2007-5352

- **16824 Windows Kernel TCP/IP/ICMP Vulnerability (MS08-001/941644) (Remote File Checking)**

A denial of service vulnerability exists in TCP/IP due to the way that Windows Kernel processes fragmented router advertisement ICMP queries. ICMP Router Discovery Protocol (RDP) is not enabled by default and is required in order to exploit this vulnerability. However, on Windows 2003 Server and on Windows XP, RDP can be turned on by a setting in DHCP or by a setting in the registry. On Windows 2000, RDP can be turned on by a setting in the registry. An anonymous attacker could exploit the vulnerability by sending specially crafted ICMP packets to a computer over the network. An attacker who successfully exploited this vulnerability could cause the computer to stop responding and automatically restart.

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

References:

* MS: MS08-001
http://www.microsoft.com/technet/security/bulletin/ms08-001.mspx
* CERT: TA08-008A
http://www.us-cert.gov/cas/techalerts/TA08-008A.html
* SECUNIA: 28297
http://secunia.com/advisories/28297

CVE Reference: CVE-2007-0066

❖ 16823 Windows Kernel TCP/IP/IGMPv3 and MLDv2 Vulnerability (MS08-001/941644) (Remote File Checking)

A remote code execution vulnerability exists in the Windows kernel due to the way that the Windows kernel handles TCP/IP structures storing the state of IGMPv3 and MLDv2 queries. Supported editions of Microsoft Windows XP, Windows Server 2003, and Windows Vista all support IGMPv3. In addition to IGMPv3, Windows Vista supports MDLv2, which adds multicast support for IPv6 networks. An anonymous attacker could exploit the vulnerability by sending specially crafted IGMPv3 and MLDv2 packets to a computer over the network. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

* MS: MS08-001
http://www.microsoft.com/technet/security/bulletin/ms08-001.mspx
* CERT: TA08-008A
http://www.us-cert.gov/cas/techalerts/TA08-008A.html
* SECUNIA: 28297
http://secunia.com/advisories/28297

CVE Reference: CVE-2007-0069

❖ 16712 Oracle Application Server - Oracle Forms component unspecified Vulnerability (oct-2006/FORM02)

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:

* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/449711/100/0/threaded
* CERT: TA06-291A
http://www.us-cert.gov/cas/techalerts/TA06-291A.html
* BID: 20588
http://www.securityfocus.com/bid/20588
* FRSIRT: ADV-2006-4065
http://www.frsirt.com/english/advisories/2006/4065
* SECTRACK: 1017077
http://securitytracker.com/id?1017077
* SECUNIA: 22396
http://secunia.com/advisories/22396

CVE Reference: CVE-2006-5365

❖ 16711 Oracle Application Server - Oracle Forms component unspecified Vulnerability (oct-2006/FORM01)

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:

* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/449711/100/0/threaded
* CERT: TA06-291A
http://www.us-cert.gov/cas/techalerts/TA06-291A.html
* BID: 20588
http://www.securityfocus.com/bid/20588
* FRSIRT: ADV-2006-4065
http://www.frsirt.com/english/advisories/2006/4065
* SECTRACK: 1017077
http://securitytracker.com/id?1017077
* SECUNIA: 22396
http://secunia.com/advisories/22396

CVE Reference: CVE-2006-5358

❖ 16710 Oracle Application Server - Oracle HTTP Server component unspecified Vulnerability (oct-2006/OHS03)

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

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

References:

* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/449711/100/0/threaded
* CERT: TA06-291A
http://www.us-cert.gov/cas/techalerts/TA06-291A.html
* BID: 20588
http://www.securityfocus.com/bid/20588
* FRSIRT: ADV-2006-4065
http://www.frsirt.com/english/advisories/2006/4065
* SECTRACK: 1017077
http://securitytracker.com/id?1017077
* SECUNIA: 22396
http://secunia.com/advisories/22396

CVE Reference: CVE-2006-5357

❖ 16709 Oracle Application Server - Oracle Single Sign-On component unspecified Vulnerability (oct-2006/SSO01)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Single Sign-On component.

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

References:

* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/449711/100/0/threaded
* CERT: TA06-291A
http://www.us-cert.gov/cas/techalerts/TA06-291A.html
* BID: 20588
http://www.securityfocus.com/bid/20588
* FRSIRT: ADV-2006-4065

http://www.frsirt.com/english/advisories/2006/4065
* SECTRACK: 1017077
http://securitytracker.com/id?1017077
* SECUNIA: 22396
http://secunia.com/advisories/22396

CVE Reference: CVE-2006-5355

❖ **16708 Oracle Application Server - Oracle HTTP Server component unspecified Vulnerability (oct-2006/OHS01)**

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

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

References:

* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/449711/100/0/threaded
* CERT: TA06-291A
http://www.us-cert.gov/cas/techalerts/TA06-291A.html
* BID: 20588
http://www.securityfocus.com/bid/20588
* FRSIRT: ADV-2006-4065
http://www.frsirt.com/english/advisories/2006/4065
* SECTRACK: 1017077
http://securitytracker.com/id?1017077
* SECUNIA: 22396
http://secunia.com/advisories/22396

CVE Reference: CVE-2006-5353

❖ **16701 Oracle Application Server - Oracle Internet Directory component unspecified Vulnerability (jan-2007/OID01)**

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

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html
* CERT: TA07-017A

http://www.us-cert.gov/cas/techalerts/TA07-017A.html
* SECTRACK: 1017522
http://securitytracker.com/id?1017522
* SECUNIA: 23794
http://secunia.com/advisories/23794
* XF: oracle-cpu-jan2007(31541)
http://xforce.iss.net/xforce/xfdb/31541

CVE Reference: CVE-2007-0288

❖ **16700 Oracle Application Server - Oracle Containers for J2EE component unspecified Vulnerability (jan-2007/OC4J08)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Containers for J2EE component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2007.html
* CERT: TA07-017A
http://www.us-cert.gov/cas/techalerts/TA07-017A.html
* SECTRACK: 1017522
http://securitytracker.com/id?1017522
* SECUNIA: 23794
http://secunia.com/advisories/23794
* XF: oracle-cpu-jan2007(31541)
http://xforce.iss.net/xforce/xfdb/31541

CVE Reference: CVE-2007-0287

New Vulnerabilities found this Week

Microsoft Patch Tuesday, January 2008

Microsoft released patches for the following 3 vulnerabilities:

Windows Kernel TCP/IP/IGMPv3 and MLDv2 Vulnerability (MS08-001/941644)

A remote code execution vulnerability exists in the Windows kernel due to the way that the Windows kernel handles TCP/IP structures storing the state of IGMPv3 and MLDv2 queries. Supported editions of Microsoft Windows XP, Windows Server 2003, and Windows Vista all support IGMPv3. In addition to IGMPv3, Windows Vista supports MDLv2, which adds multicast support for IPv6 networks. An anonymous attacker could exploit the vulnerability by sending specially crafted IGMPv3 and MLDv2 packets to a computer over the network. An attacker who successfully exploited this vulnerability could take

complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Windows Kernel TCP/IP/ICMP Vulnerability (MS08-001/941644)

A denial of service vulnerability exists in TCP/IP due to the way that Windows Kernel processes fragmented router advertisement ICMP queries. ICMP Router Discovery Protocol (RDP) is not enabled by default and is required in order to exploit this vulnerability. However, on Windows 2003 Server and on Windows XP, RDP can be turned on by a setting in DHCP or by a setting in the registry. On Windows 2000, RDP can be turned on by a setting in the registry. An anonymous attacker could exploit the vulnerability by sending specially crafted ICMP packets to a computer over the network. An attacker who successfully exploited this vulnerability could cause the computer to stop responding and automatically restart.

LSASS Bypass Vulnerability (MS08-002/943485)

An elevation of privilege vulnerability exists in the Microsoft Windows Local Security Authority Subsystem Service (LSASS) due to its improper handling of local procedure call (LPC) requests. The vulnerability could allow an attacker to run code with elevated privileges. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

References:
http://www.microsoft.com/technet/security/bulletin/ms08-001.mspx
http://www.microsoft.com/technet/security/Bulletin/MS08-002.mspx
http://descriptions.securescout.com/tc/16823
http://descriptions.securescout.com/tc/16824
http://descriptions.securescout.com/tc/16825

AOL Radio AOLMediaPlaybackControl.exe Buffer Overflow Vulnerability

“execution of arbitrary code”

Will Dormann has reported a vulnerability in AOL Radio, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in AOLMediaPlaybackControl.exe and can be exploited to cause a stack-based buffer overflow by e.g. using the "AppendFileToPlayList()" method of the AmpX ActiveX control.

Successful exploitation allows execution of arbitrary code.
References:
http://www.kb.cert.org/vuls/id/568681

IMP Mail Deletion Security Bypass Vulnerability

“delete e-mail messages; purge deleted mails”

Secunia Research has discovered a vulnerability in IMP Webmail Client and Horde Groupware Webmail Edition, which can be exploited by malicious people to bypass certain security restrictions and manipulate data.

The HTML filter does not filter out <frame> and <frameset> HTML elements. Additionally,

the application allows users to perform certain actions via HTTP requests without performing any validity checks to verify the request. This can be exploited to (a) delete an arbitrary number of e-mail messages by referencing their numeric IDs and (b) purge deleted mails, when the victim opens a malicious HTML mail.

Successful exploitation requires that the victim opens the HTML part of a malicious message.

The vulnerability is confirmed in IMP version 4.1.5 with Horde version 3.1.5 and also reported in Horde Groupware Webmail Edition 1.0.3. Other versions may also be affected.

References:
http://secunia.com/secunia_research/2007-102/

Linksys WRT54GL Cross-Site Request Forgery
"cross-site request forgery attacks"

Tomaz Bratusa has reported a vulnerability in Linksys WRT54GL, which can be exploited by malicious people to conduct cross-site request forgery attacks.

The vulnerability is caused due to the device allowing users to perform certain actions via HTTP requests without performing any validity checks to verify the request. This can be exploited to e.g. disable the firewall by enticing a logged-in administrator to visit a malicious site.

The vulnerability affects firmware versions 4.30.11 and prior.

References:
http://archives.neohapsis.com/archives/bugtraq/2008-01/0063.html

VMware ESX Server Multiple Security Updates
"Denial of Service"

VMware has issued an update for VMware ESX Server. This fixes some vulnerabilities, which can be exploited by malicious, local users to perform actions with escalated privileges and by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

References:
http://lists.vmware.com/pipermail/security-announce/2008/000002.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