

Table of Contents

[Product Focus](#)

[This Week in Review](#)

[Top Security News Stories this Week](#)

[New Vulnerabilities Tested in SecureScout](#)

[New Vulnerabilities found this Week](#)

Product Focus

[Nimda Worm Scanner](#) - The S4 Nimda 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 MS IE Mime Header Flaw (MS01-020) or have been infected by the Nimda Worm.

Download Here:

<http://www.netvigilance.com/productdownloads?productname=nimdawormscanner>

This Week in Review

IT spendings during the crisis. Enjoy a period with less spam. Hope that Obama will better cybersecurity. Google provide spam calculator.

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

• Top five IT spending priorities for hard times

November 19, 2008 (InfoWorld) No company is immune to the economy's ebb and flow. So it's no surprise that, in the face of a fearsome downturn, IT shops are scrambling to figure out where they should cut.

Just how severe is the impact of the economy on IT? Find out in "Is tech in more trouble than we think?"

At brokerage and investment banking firm Morgan Keegan, for example, CIO John Threadgill acknowledges that he has to "come up with better reasons" for the technologies to which he allocates IT resources. But after he eliminates or delays costs where feasible, Threadgill and his CIO colleagues must continue investing in certain areas, no matter how crazily the economy bounces up or down. "We'll continue to spend where we need to," says Threadgill.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9120838&source=rss_topic1

• Spam levels remain down following McColo shutdown

Though worldwide spam levels are still diminished in the wake of the McColo web hosting-company shutdown, it may only be a matter of time before they come roaring back.

"This is the most significant single event in the fight against spam we have ever seen," said Phil Hay, lead threat analyst with the TRACE Team. "Unfortunately we do not expect this situation to last."

Simon Heron, internet security analyst at Network Box, said: "We've also seen a significant drop in emails containing viruses and phishing attacks. This indicates that McColo's servers were also used to distribute malicious emails containing viruses, and not just the usual junk marketing mail."

SC Magazine

Full Story :

<http://www.scmagazineus.com/Spam-levels-remain-down-following-McColo-shutdown/article/121298/>

• Feds urged to provide cybersecurity incentives

November 19, 2008 (IDG News Service) President-elect Barack Obama needs to take a new approach to cybersecurity, with the government providing incentives for private businesses to adopt security measures, a cybersecurity group said.

The Bush administration's 2002 National Strategy to Secure Cyber Space and later efforts contained "no serious attempt" to address incentives needed for private business to invest in cybersecurity, the report said.

A new ISA report, "The Cyber Security Social Contract" (download PDF), released Tuesday, recommends that the U.S. government establish incentives -- tax breaks, small-business loans or lawsuit protection -- for private companies to invest in cybersecurity.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9120868&source=rss_topic1

• How much does spam cost you? Google will calculate

November 19, 2008 (IDG News Service) How much is spam costing your company? Google Inc. unveiled a nifty little calculator on Wednesday to help you add it up.

To figure out the cost of spam, you enter things like the number of workers at your company, how much you pay them and how much spam they have to deal with, and presto: Google figures out how many days (and dollars) in lost productivity this represents. Of course, it also tells you how long it would take for Google's service to pay for itself at your shop.

Last year, Nucleus Research Inc. reported that spam costs U.S. companies \$712 per employee each year. A \$31,000-per-year employee spending 16 seconds each on 21 spam messages per day would cost about this much, according to Google's calculator. That adds up to about \$70 billion per year in lost productivity, Nucleus said.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9120872&source=rss_topic1

New Vulnerabilities Tested in SecureScout

• 16767 Oracle Application Server - Web Cache component unspecified Vulnerability (oct-2005/AS12)

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

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html>

* CERT: TA05-292A

<http://www.us-cert.gov/cas/techalerts/TA05-292A.html>

* CERT-VN: VU#210524

<http://www.kb.cert.org/vuls/id/210524>

* BID: 15134

<http://www.securityfocus.com/bid/15134>

* SECUNIA: 17250

<http://secunia.com/advisories/17250>

CVE Reference:

CVE-2005-3453 (cve.mitre.org, nvd.nist.gov)

• 16768 Oracle Application Server - Web Cache component unspecified Vulnerability (oct-2005/AS13)

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

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html>

* CERT: TA05-292A

<http://www.us-cert.gov/cas/techalerts/TA05-292A.html>

* CERT-VN: VU#210524

<http://www.kb.cert.org/vuls/id/210524>

* BID: 15134

<http://www.securityfocus.com/bid/15134>

* SECUNIA: 17250

<http://secunia.com/advisories/17250>

CVE Reference:

CVE-2005-3452 (cve.mitre.org, nvd.nist.gov)

• 16769 Oracle Application Server - Web Cache component unspecified Vulnerability (oct-2005/AS14)

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

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html>

* CERT: TA05-292A

<http://www.us-cert.gov/cas/techalerts/TA05-292A.html>

* CERT-VN: VU#210524

<http://www.kb.cert.org/vuls/id/210524>

* BID: 15134

<http://www.securityfocus.com/bid/15134>

* SECUNIA: 17250

<http://secunia.com/advisories/17250>

CVE Reference:

CVE-2005-3453 (cve.mitre.org, nvd.nist.gov)

• 16770 Oracle Application Server - Oracle Workflow Cartridge component unspecified Vulnerability (oct-2005/AS15)

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

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html>

CVE Reference:

• 16771 Oracle Application Server - Oracle Workflow Cartridge component unspecified Vulnerability (oct-2005/AS16)

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

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html>

CVE Reference:

• **16772 Oracle Application Server - Oracle Workflow Cartridge component unspecified Vulnerability (oct-2005/AS17)**

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

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html>

CVE Reference:

• **16773 Oracle Application Server - Oracle Workflow Cartridge component unspecified Vulnerability (oct-2005/AS18)**

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

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html>

CVE Reference:

• **16774 Oracle Application Server - Oracle Workflow Cartridge component unspecified Vulnerability (oct-2005/AS19)**

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

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html>

CVE Reference:

• **18170 Apache HTTP Server, Cross-site request forgery (CSRF) vulnerability in the balancer-manager in mod_proxy_balancer**

Cross-site request forgery (CSRF) vulnerability in the balancer-manager in mod_proxy_balancer for Apache HTTP Server 2.2.x allows remote attackers to gain privileges via unspecified vectors.

The issue has been fixed in version 2.2.9.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **Medium**

References:

* BUGTRAQ: 20080110 SecurityReason - Apache2 CSRF, XSS, Memory Corruption and Denial of Service Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/486169/100/0/threaded>

* BUGTRAQ: 20080729 rPSA-2008-0236-1 httpd mod_ssl

<http://www.securityfocus.com/archive/1/archive/1/494858/100/0/threaded>

* CONFIRM:

<http://support.apple.com/kb/HT3216>

* APPLE: APPLE-SA-2008-10-09

<http://lists.apple.com/archives/security-announce/2008/Oct/msg00001.html>

* GENTOO: GLSA-200807-06

<http://security.gentoo.org/glsa/glsa-200807-06.xml>

* BID: 27236

<http://www.securityfocus.com/bid/27236>

* FRSIRT: ADV-2008-2780

<http://www.frsirt.com/english/advisories/2008/2780>

* SECUNIA: 31026

<http://secunia.com/advisories/31026>

* SECUNIA: 32222

<http://secunia.com/advisories/32222>

* SREASON: 3523

<http://securityreason.com/securityalert/3523>

CVE Reference:

CVE-2007-6420 (cve.mitre.org, nvd.nist.gov)

• 18171 Apache mod_proxy Interim Responses Denial of Service

A vulnerability has been reported in the Apache mod_proxy module, which potentially can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the "ap_proxy_http_process_response()" function when forwarding interim responses. This can be exploited to consume large amounts of memory by tricking mod_proxy into sending an overly large number of interim responses to the client.

The vulnerability is reported in versions 2.2.x lower than 2.2.9.

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

References:

* BUGTRAQ: 20080110 SecurityReason - Apache2 CSRF, XSS, Memory Corruption and Denial of Service Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/486169/100/0/threaded>

* BUGTRAQ: 20080729 rPSA-2008-0236-1 httpd mod_ssl

<http://www.securityfocus.com/archive/1/archive/1/494858/100/0/threaded>

* CONFIRM:

<http://support.apple.com/kb/HT3216>

* APPLE: APPLE-SA-2008-10-09

<http://lists.apple.com/archives/security-announce/2008/Oct/msg00001.html>

* GENTOO: GLSA-200807-06

<http://security.gentoo.org/glsa/glsa-200807-06.xml>

* BID: 27236

<http://www.securityfocus.com/bid/27236>

* FRSIRT: ADV-2008-2780

<http://www.frsirt.com/english/advisories/2008/2780>

* SECUNIA: 31026

<http://secunia.com/advisories/31026>

* SECUNIA: 32222

<http://secunia.com/advisories/32222>

* SREASON: 3523

<http://securityreason.com/securityalert/3523>

CVE Reference:

CVE-2008-2364 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2008-5100 Microsoft CVSS 2.0 Score = 10.0

The strong name (SN) implementation in Microsoft .NET Framework 2.0.50727 relies on the digital signature Public Key Token embedded in the pathname of a DLL file instead of the digital signature of this file itself, which makes it easier for attackers to bypass Global Assembly Cache (GAC) and Code Access Security (CAS) protection mechanisms, aka MSRC ticket MSRC8566gs.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/498311/100/0/threaded>

MISC: <http://www.applicationsecurity.co.il/LinkClick.aspx?fileticket=ycIS1bewMBI%3d&tabid=161&mid=555>

MISC: <http://www.applicationsecurity.co.il/.NET-Framework-Rootkits.aspx>

CVE Reference: [CVE-2008-5100](#)

• **CVE-2008-5112 Microsoft CVSS 2.0 Score = 5.0**

The LDAP server in Active Directory in Microsoft Windows 2000 SP4 and Server 2003 SP1 and SP2 responds differently to a failed bind attempt depending on whether the user account exists and is permitted to login, which allows remote attackers to enumerate valid usernames via a series of LDAP bind requests, as demonstrated by ldapuserenum.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

BID: <http://www.securityfocus.com/bid/32305>

MISC: <http://www.portcullis-security.com/294.php>

MISC: <http://labs.portcullis.co.uk/application/ldapuserenum/>

CVE Reference: [CVE-2008-5112](#)

• **CVE-2008-5179 Microsoft CVSS 2.0 Score = 5.0**

Unspecified vulnerability in Microsoft Office Communications Server (OCS), Office Communicator, and Windows Live Messenger allows remote attackers to cause a denial of service (crash) via a crafted Real-time Transport Control Protocol (RTCP) receiver report packet.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

XF: <http://xforce.iss.net/xforce/xfdb/46670>

MISC: <http://www.voipshield.com/research-details.php?id=132>

BID: <http://www.securityfocus.com/bid/32341>

CVE Reference: [CVE-2008-5179](#)

• **CVE-2008-5180 Microsoft CVSS 2.0 Score = 5.0**

Microsoft Communicator allows remote attackers to cause a denial of service (memory consumption) via a large number of SIP INVITE requests, which trigger the creation of many sessions.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

XF: <http://xforce.iss.net/xforce/xfdb/46673>

MISC: <http://www.voipshield.com/research-details.php?id=133>

CVE Reference: [CVE-2008-5180](#)

• **CVE-2008-5181 Microsoft CVSS 2.0 Score = 5.0**

Microsoft Communicator allows remote attackers to cause a denial of service (application or device outage) via instant messages containing large numbers of emoticons.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

XF: <http://xforce.iss.net/xforce/xfdb/46671>

MISC: <http://www.voipshield.com/research-details.php?id=131>

CVE Reference: [CVE-2008-5181](#)

• **CVE-2008-5120 HP CVSS 2.0 Score = 10.0**

Stack-based buffer overflow in the Process Software MultiNet finger service (aka FINGERD) for HP OpenVMS 8.3 allows remote attackers to execute arbitrary code via a long request string.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

BID: <http://www.securityfocus.com/bid/30589>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/495207/100/0/threaded>

CVE Reference: [CVE-2008-5120](#)

• CVE-2008-4415 HP CVSS 2.0 Score = 9.0

Unspecified vulnerability in HP Service Manager (HPSM) before 7.01.71 allows remote authenticated users to execute arbitrary code via unknown vectors.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

BID: <http://www.securityfocus.com/bid/32272>

HP: <http://marc.info/?l=bugtraq&m=122652356130271&w=2>

HP: <http://marc.info/?l=bugtraq&m=122652356130271&w=2>

CVE Reference: [CVE-2008-4415](#)

• CVE-2008-5134 Linux CVSS 2.0 Score = 10.0

Buffer overflow in the lbs_process_bss function in drivers/net/wireless/libertas/scan.c in the libertas subsystem in the Linux kernel before 2.6.27.5 allows remote attackers to have an unknown impact via an "invalid beacon/probe response."

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=470761

MLIST: <http://openwall.com/lists/oss-security/2008/11/11/2>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/stable/linux-2.6.27.y.git;a=commit;h=48735d8d8bd701b1e0cd3d49c21e5e385ddcb>

MLIST: <http://article.gmane.org/gmane.linux.kernel.wireless.general/23049>

CVE Reference: [CVE-2008-5134](#)

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