

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

[Messenger Service Vulnerability Scanner](#) - The S4 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).

Download Here:

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

This Week in Review

Hackers utilize president election. Researchers able to crack WPA encryption. e-payments a dangerous bussines. Internet crime today.

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

• Hackers begin malware barrage soon after Obama elected

Hours after Barack Obama was elected president of the United States, cybercriminals began capitalizing on the historic news by delivering a barrage of malware-laden spam to users worldwide.

The emails were typical social-engineering ploys: They claimed to contain a video of an "amazing speech" by the president-elect but actually included a link to a trojan, said Graham Cluley, senior technology consultant at endpoint security firm Sophos.

"They wasted no time at all," Cluley told SCMagazineUS.com. "It's just taking advantage of Obama-mania."

SC Magazine

Full Story :

<http://www.scmagazineus.com/Hackers-begin-malware-barrage-soon-after-Obama-elected/article/120469/>

• **Once thought safe, WPA Wi-Fi encryption is cracked**

November 6, 2008 (IDG News Service) Security researchers say they've developed a way to partially crack the Wi-Fi Protected Access (WPA) encryption standard used to protect data on many wireless networks.

To do this, Tews and his co-researcher Martin Beck found a way to break the Temporal Key Integrity Protocol (TKIP) key, used by WPA, in a relatively short amount of time: 12 to 15 minutes, according to Dragos Ruiu, the PacSec conference's organizer.

Security experts had known that TKIP could be cracked using what's known as a dictionary attack. Using massive computational resources, the attacker essentially cracks the encryption by making an extremely large number of educated guesses as to what key is being used to secure the wireless data.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9119258&source=rss_topic1

• **Opinion: Card breaches shake faith in e-payments**

November 6, 2008 (IDG News Service) In the past three months, all three of my payments cards -- one credit card and two debit cards -- have been compromised.

The card breaches are particularly disturbing since I cover computer security. So what happened? I still have no clue. Investigating a card breach as a consumer, or a journalist, is a black hole.

Point-of-sale devices can be modified to record card details. Unscrupulous employees can also steal information during merchant transactions. All of the methods can allow a hacker to eventually use the details and attempt an online transaction, known as card-not-present fraud.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9119359&source=rss_topic1

• **Three ways Internet crime has changed**

November 3, 2008 (CSO) Gone are the days when most hackers were looking for fame with a splashy, large-scale attack on a network that made headlines. Today's cybercriminals are quietly taking over vulnerable web sites as part of an elaborate process in the underground economy.

One trend highlighted in the report change is the motivation of hackers, according to the data. "The trend has moved from hacking attempts being done for notoriety to hacking for criminal intent and fraud," said Grant Geyer, vice president of Symantec Managed Security Services.

Botnets spearhead for-profit hacker activities

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9118882&source=rss_topic1

New Vulnerabilities Tested in SecureScout

• **16617 Apache HTTP Server, Signals to arbitrary processes Vulnerability**

The Apache HTTP server did not verify that a process was an Apache child process before sending it signals. A local attacker with the ability to run scripts on the HTTP server could manipulate the scoreboard and cause arbitrary processes to be terminated which could lead to a denial of service.

The vulnerability has been fixed in versions 2.2.6, 2.0.61 and 1.3.39.

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

References:

* BUGTRAQ: 20070529 Apache httpd vulnerabilities

<http://www.securityfocus.com/archive/1/archive/1/469899/100/0/threaded>

* BUGTRAQ: 20070619 Apache Prefork MPM vulnerabilities - Report

<http://www.securityfocus.com/archive/1/archive/1/471832/100/0/threaded>

* MLIST: [apache-httpd-dev] 20070622 Re: PID table changes (was Re: svn commit: r547987 - in /httpd/httpd/trunk)
<http://marc.info/?l=apache-httpd-dev&m=118252946632447&w=2>

* MLIST: [apache-httpd-dev] 20070629 Re: [PATCH] pid safety checks for 2.2.x
http://mail-archives.apache.org/mod_mbox/httpd-dev/200706.mbox/%3c20070629141032.GA15192@redhat.com%3e

* MISC:
http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=245111

* CONFIRM:
<http://svn.apache.org/viewvc?view=rev&revision=547987>

* CONFIRM:
http://httpd.apache.org/security/vulnerabilities_13.html

* CONFIRM:
http://httpd.apache.org/security/vulnerabilities_20.html

* CONFIRM:
http://httpd.apache.org/security/vulnerabilities_22.html

* CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2007-353.htm>

* CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2007-363.htm>

* AIXAPAR: PK50467
<http://www-1.ibm.com/support/search.wss?rs=0&q=PK50467&apar=only>

* MANDRIVA: MDKSA-2007:140
<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:140>

* MANDRIVA: MDKSA-2007:142
<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:142>

* REDHAT: RHSA-2007:0556
<http://rhn.redhat.com/errata/RHSA-2007-0556.html>

* REDHAT: RHSA-2007:0557
<http://www.redhat.com/support/errata/RHSA-2007-0557.html>

* REDHAT: RHSA-2007:0662
<http://www.redhat.com/support/errata/RHSA-2007-0662.html>

* SGI: 20070701-01-P
<ftp://patches.sgi.com/support/free/security/advisories/20070701-01-P.asc>

* UBUNTU: USN-499-1
<http://www.ubuntu.com/usn/usn-499-1>

* BID: 24215
<http://www.securityfocus.com/bid/24215>

* FRSIRT: ADV-2007-2727
<http://www.frsirt.com/english/advisories/2007/2727>

* FRSIRT: ADV-2007-3100
<http://www.frsirt.com/english/advisories/2007/3100>

* SECTRACK: 1018304
<http://www.securitytracker.com/id?1018304>

* SECUNIA: 25827
<http://secunia.com/advisories/25827>

* SECUNIA: 25830
<http://secunia.com/advisories/25830>

* SECUNIA: 25920
<http://secunia.com/advisories/25920>

* SECUNIA: 26211
<http://secunia.com/advisories/26211>

* SECUNIA: 26273
<http://secunia.com/advisories/26273>

* SECUNIA: 26443
<http://secunia.com/advisories/26443>

* SECUNIA: 26508
<http://secunia.com/advisories/26508>

* SECUNIA: 26611
<http://secunia.com/advisories/26611>

* SECUNIA: 26759
<http://secunia.com/advisories/26759>

* SREASON: 2814
<http://securityreason.com/securityalert/2814>

CVE Reference:

CVE-2007-3304 (cve.mitre.org, nvd.nist.gov)

• **16758 Oracle Application Server - Oracle HTTP Server component unspecified Vulnerability (oct-2005/AS03)**

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:

- * 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>
- * CERT-VN: VU#890940
<http://www.kb.cert.org/vuls/id/890940>
- * BID: 15134
<http://www.securityfocus.com/bid/15134>
- * SECUNIA: 17250
<http://secunia.com/advisories/17250>

CVE Reference:

CVE-2005-3445 (cve.mitre.org, nvd.nist.gov)

• **16759 Oracle Application Server - Oracle HTTP Server component unspecified Vulnerability (oct-2005/AS04)**

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:

- * 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-2005-3450 (cve.mitre.org, nvd.nist.gov)

• **16760 Oracle Application Server - Oracle HTTP Server component unspecified Vulnerability (oct-2005/AS05)**

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:

- * 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>
- * CERT-VN: VU#890940
<http://www.kb.cert.org/vuls/id/890940>
- * BID: 15134
<http://www.securityfocus.com/bid/15134>
- * SECUNIA: 17250
<http://secunia.com/advisories/17250>

CVE Reference:

CVE-2005-3445 (cve.mitre.org, nvd.nist.gov)

• **16761 Oracle Application Server - Oracle Internet Directory component unspecified Vulnerability (oct-2005/AS06)**

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

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

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-2005-3446 (cve.mitre.org, nvd.nist.gov)

• **16762 Oracle Application Server - Oracle Internet Directory component unspecified Vulnerability (oct-2005/AS07)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Internet Directory 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>
- * CERT-VN: VU#376756
<http://www.kb.cert.org/vuls/id/376756>
- * CERT-VN: VU#512716
<http://www.kb.cert.org/vuls/id/512716>
- * BID: 15134
<http://www.securityfocus.com/bid/15134>
- * SECUNIA: 17250
<http://secunia.com/advisories/17250>

CVE Reference:

CVE-2005-3449 (cve.mitre.org, nvd.nist.gov)

• **16763 Oracle Application Server - Oracle Single Sign-On component unspecified Vulnerability (oct-2005/AS08)**

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: **Low**

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-2005-3447 (cve.mitre.org, nvd.nist.gov)

● **16764 Oracle Application Server - Report Server component unspecified Vulnerability (oct-2005/AS09)**

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

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

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>
- * CERT-VN: VU#376756
<http://www.kb.cert.org/vuls/id/376756>
- * CERT-VN: VU#512716
<http://www.kb.cert.org/vuls/id/512716>
- * BID: 15134
<http://www.securityfocus.com/bid/15134>
- * SECUNIA: 17250
<http://secunia.com/advisories/17250>

CVE Reference:

CVE-2005-3449 (cve.mitre.org, nvd.nist.gov)

● **16765 Oracle Application Server - SQL*ReportWriter component unspecified Vulnerability (oct-2005/AS10)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server SQL*ReportWriter 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>
- * CERT-VN: VU#171364
<http://www.kb.cert.org/vuls/id/171364>
- * BID: 15134
<http://www.securityfocus.com/bid/15134>
- * SECUNIA: 17250
<http://secunia.com/advisories/17250>

CVE Reference:

CVE-2005-3451 (cve.mitre.org, nvd.nist.gov)

● **16766 Oracle Application Server - Web Cache component unspecified Vulnerability (oct-2005/AS11)**

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>
- * CERT-VN: VU#376756
<http://www.kb.cert.org/vuls/id/376756>
- * CERT-VN: VU#512716
<http://www.kb.cert.org/vuls/id/512716>
- * BID: 15134

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

* SECUNIA: 17250

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

CVE Reference:

CVE-2005-3449 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2008-4927 Microsoft CVSS 2.0 Score = 4.3

Microsoft Windows Media Player (WMP) 9.0 through 11 allows user-assisted attackers to cause a denial of service (application crash) via a malformed (1) MIDI or (2) DAT file, related to "MThd Header Parsing." NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.

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

References:

BID: <http://www.securityfocus.com/bid/32077>

CVE Reference: [CVE-2008-4927](#)

• CVE-2008-4413 HP CVSS 2.0 Score = 6.2

Unspecified vulnerability in HP System Management Homepage (SMH) 2.2.6 and earlier on HP-UX B.11.11 and B.11.23, and SMH 2.2.6 and 2.2.8 and earlier on HP-UX B.11.23 and B.11.31, allows local users to gain "unauthorized access" via unknown vectors, possibly related to temporary file permissions.

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

References:

FRSIRT: <http://www.frsirt.com/english/advisories/2008/2999>

SECUNIA: <http://secunia.com/advisories/32544>

HP: <http://marc.info/?l=bugtraq&m=122581539223159&w=2>

CVE Reference: [CVE-2008-4413](#)

• CVE-2008-4963 Cisco CVSS 2.0 Score = 7.1

Unspecified vulnerability in the VLAN Trunking Protocol (VTP) implementation on Cisco IOS and CatOS, when the VTP operating mode is not transparent, allows remote attackers to cause a denial of service (device reload or hang) via a crafted VTP packet.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/46346>

BID: <http://www.securityfocus.com/bid/32120>

CISCO: http://www.cisco.com/en/US/products/products_security_response09186a0080a231cf.html

SECTRAK: <http://securitytracker.com/id?1021143>

CVE Reference: [CVE-2008-4963](#)

• CVE-2008-4910 Sun CVSS 2.0 Score = 10.0

The BasicService in Sun Java Web Start allows remote attackers to execute arbitrary programs on a client machine via a file:// URL argument to the showDocument method.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/46119>

BID: <http://www.securityfocus.com/bid/31916>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/497972/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/497799/100/0/threaded>

CVE Reference: [CVE-2008-4910](#)

• **CVE-2008-2992 Adobe CVSS 2.0 Score = 9.3**

Stack-based buffer overflow in Adobe Acrobat and Reader 8.1.2 allows remote attackers to execute arbitrary code via a PDF file containing a crafted format string in the util.printf JavaScript function.

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

References:

BID: <http://www.securityfocus.com/bid/32091>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/498032/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/498027/100/0/threaded>

MISC: <http://www.coresecurity.com/content/adobe-reader-buffer-overflow>

MISC: http://secunia.com/secunia_research/2008-14/

SECUNIA: <http://secunia.com/advisories/29773>

CVE Reference: [CVE-2008-2992](#)

• **CVE-2008-4812 Adobe CVSS 2.0 Score = 9.3**

Array index error in Adobe Reader and Acrobat, and the Explorer extension (aka AcroRd32Info), 8.1.2, 8.1.1, and earlier allows remote attackers to execute arbitrary code via a crafted PDF document that triggers an out-of-bounds write, related to parsing of Type 1 fonts.

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

References:

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb08-19.html>

BID: <http://www.securityfocus.com/bid/32100>

IDEFENSE: <http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=755>

CVE Reference: [CVE-2008-4812](#)

• **CVE-2008-4813 Adobe CVSS 2.0 Score = 9.3**

Adobe Reader and Acrobat 8.1.2 and earlier allow remote attackers to execute arbitrary code via a crafted PDF document that (1) performs unspecified actions on a Collab object that trigger memory corruption, related to a GetCosObj method; or (2) contains a malformed PDF object that triggers memory corruption during parsing.

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

References:

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb08-19.html>

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-08-074/>

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-08-073/>

BID: <http://www.securityfocus.com/bid/32100>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/498057/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/498056/100/0/threaded>

CVE Reference: [CVE-2008-4813](#)

• **CVE-2008-4814 Adobe CVSS 2.0 Score = 9.3**

Unspecified vulnerability in a JavaScript method in Adobe Reader and Acrobat 8.1.2 and earlier allows remote attackers to execute arbitrary code via unknown vectors, related to an "input validation issue."

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

References:

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb08-19.html>

MISC: http://www.skyrecon.com/index.php?option=com_content&task=view&id=302&Itemid=124

BID: <http://www.securityfocus.com/bid/32100>

CVE Reference: [CVE-2008-4814](#)

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