

2009 Issue #19

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

[Winny \(WinNY\) software Scanner](#) - The S4 Winny Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if the peer-to-peer software Winny is installed and running.

Download Here:

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

This Week in Review

Governments calling for help. NERC looking at new 'Critical Infrastructure Protection Act'. Botnets are swelling dramatically. One botnet infiltrated by the 'good guys'.

Enjoy reading & Stay safe.

Call or email netVigilance to get an update on SecureScout.

(503) 524 5758 or [sales@netVigilance.com](mailto:sales@netvigilance.com)

Top Security News Stories this Week

• Call for a global cyberthreat solution

Governments around the world must join together to create a transnational solution to cyberthreats, according to a report published Wednesday by Deloitte Touche Tohmatsu.

The report "Cybersecurity: Everybody's Imperative. Protecting our economies, governments, and citizens," concludes that each government must partner with the private sector, citizens, and other governments to work on a holistic solution that goes beyond just technology to combat cyberthreats. Because of the global nature of the threats, uniform standards of protection are needed, the report says.

"It matters little if an individual nation or alliance has advanced its cybersecurity ahead of the rest," the report asserts.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Call-for-a-global-cyberthreat-solution/article/136302/>

• **NERC president: Emergency cybersecurity help needed**

Efforts of the North American Electric Reliability Corp. (NERC) to secure the nation's power grid against cyber threats cannot substitute for additional emergency authority at the federal level, urged Richard Sergel, president and CEO of NERC, in testimony during a Senate hearing on cybersecurity Tuesday.

"The federal government should be given additional, carefully crafted emergency authority to address specific, imminent security threats," Sergel said.

Sergel said NERC supports legislation introduced last week, called The Critical Infrastructure Protection Act. The legislation would give the Federal Energy Regulatory Commission (FERC) authority to issue emergency rules or orders if a cyber threat is perceived as imminent (FERC is the U.S. agency responsible for overseeing electric rates and natural gas pricing).

SC Magazine

Full Story :

<http://www.scmagazineus.com/NERC-president-Emergency-cybersecurity-help-needed/article/136477/>

• **Computer bot profusion swells dramatically**

In the past three months, twelve million new computers have joined botnets, according to data from the latest quarterly McAfee Threats Report.

Typically, March is a record month for spam; this year it was well off its normally torrid pace. In 2008, there were an average of 153 billion messages daily, but during this year, March averaged only about 100 billion messages a day.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Computer-bot-profusion-swells-dramatically/article/136292/>

• **Researchers hijack control of Torpig botnet**

A group of researchers at the University of California, Santa Barbara, have infiltrated the Torpig botnet, which was found to be in control of hundreds of thousands of computers that were volunteering gigabytes of sensitive information.

Torpig is an advanced piece of crimeware, typically associated with bank account and credit card theft, according to these researchers, who work in the university's Department of Computer Science. Torpig uses a C&C technique that has also been adapted by the Conficker botmasters. That is, each infected bot periodically generates a list of domains to contact. The first server that sends a valid C&C reply is considered genuine.

Among their findings, the researchers learned that typical evaluations of botnet sizes, based on the count of distinct IPs, might be overestimated.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Researchers-hijack-control-of-Torpig-botnet/article/136207/>

New Vulnerabilities Tested in SecureScout

• **13703 Oracle Database Server - Workspace Manager component unspecified Vulnerability (apr-2009/CVE-2009-0986)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Workspace Manager" component.

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>

* CERT: TA09-105A

<http://www.us-cert.gov/cas/techalerts/TA09-105A.html>

* OSVDB: 53735

<http://osvdb.org/53735>

* SECTRAK: 1022052

<http://www.securitytracker.com/id?1022052>

* SECUNIA: 34693

<http://secunia.com/advisories/34693>

CVE Reference:

CVE-2009-0986 (cve.mitre.org, nvd.nist.gov)

• **13704 Oracle Database Server - Cluster Ready Services component unspecified Vulnerability (apr-2009/CVE-2009-0973)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Cluster Ready Services" component.

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>

* CERT: TA09-105A

<http://www.us-cert.gov/cas/techalerts/TA09-105A.html>

* OSVDB: 53736

<http://osvdb.org/53736>

* SECTRAK: 1022052

<http://www.securitytracker.com/id?1022052>

* SECUNIA: 34693

<http://secunia.com/advisories/34693>

CVE Reference:

CVE-2009-0973 (cve.mitre.org, nvd.nist.gov)

• **13705 Oracle Database Server - Listener component unspecified Vulnerability (apr-2009/CVE-2009-0991)**

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

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>

* CERT: TA09-105A

<http://www.us-cert.gov/cas/techalerts/TA09-105A.html>

* OSVDB: 53737

<http://osvdb.org/53737>

* SECTRAK: 1022052

<http://www.securitytracker.com/id?1022052>

* SECUNIA: 34693

<http://secunia.com/advisories/34693>

* XF: oracledatabase-tnslistener-dos(50026)

<http://xforce.iss.net/xforce/xfdb/50026>

CVE Reference:

CVE-2009-0991 (cve.mitre.org, nvd.nist.gov)

• **13706 Oracle Database Server - Application Express component unspecified Vulnerability (apr-2009/CVE-2009-0981)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Application Express" component.

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>

* CERT: TA09-105A

<http://www.us-cert.gov/cas/techalerts/TA09-105A.html>

* OSVDB: 53738

<http://osvdb.org/53738>

* SECTRAK: 1022052

<http://www.securitytracker.com/id?1022052>

* SECUNIA: 34693

<http://secunia.com/advisories/34693>

CVE Reference:

CVE-2009-0981 (cve.mitre.org, nvd.nist.gov)

• **13707 Oracle Database Server - Database Vault component unspecified Vulnerability (apr-2009/CVE-2009-0997)**

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

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>

* CERT: TA09-105A

<http://www.us-cert.gov/cas/techalerts/TA09-105A.html>

* OSVDB: 53739

<http://osvdb.org/53739>

* SECTRAK: 1022052

<http://www.securitytracker.com/id?1022052>

* SECUNIA: 34693

<http://secunia.com/advisories/34693>

CVE Reference:

CVE-2009-0997 (cve.mitre.org, nvd.nist.gov)

• **13708 Oracle Database Server - Password Policy component unspecified Vulnerability (apr-2009/CVE-2009-0988)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Password Policy" component.

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>

* CERT: TA09-105A

<http://www.us-cert.gov/cas/techalerts/TA09-105A.html>

* OSVDB: 53740

<http://osvdb.org/53740>

* SECTRAK: 1022052

<http://www.securitytracker.com/id?1022052>

* SECUNIA: 34693

<http://secunia.com/advisories/34693>

CVE Reference:

CVE-2009-0988 (cve.mitre.org, nvd.nist.gov)

• **18365 Oracle Application Server - OPMN component unspecified Vulnerability (apr-2009/CVE-2009-0993)**

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

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

References:

* BUGTRAQ: 20090414 ZDI-09-017: Oracle Applications Server 10g Format String Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/502683/100/0/threaded>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-09-017>

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>

* CERT: TA09-105A

<http://www.us-cert.gov/cas/techalerts/TA09-105A.html>

* SECTRAK: 1022055

<http://www.securitytracker.com/id?1022055>

- * SECUNIA: 34693
<http://secunia.com/advisories/34693>
- * XF: oracle-appserver-opmn-unspecified(50030)
<http://xforce.iss.net/xforce/xfdb/50030>

CVE Reference:

CVE-2009-0993 (cve.mitre.org, nvd.nist.gov)

• **18366 Oracle Application Server - BI Publisher component unspecified Vulnerability (apr-2009/CVE-2009-0989)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server "BI Publisher" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>
- * CERT: TA09-105A
<http://www.us-cert.gov/cas/techalerts/TA09-105A.html>
- * OSVDB: 53742
<http://osvdb.org/53742>
- * SECTRACK: 1022055
<http://www.securitytracker.com/id?1022055>
- * SECUNIA: 34693
<http://secunia.com/advisories/34693>

CVE Reference:

CVE-2009-0989 (cve.mitre.org, nvd.nist.gov)

• **18367 Oracle Application Server - BI Publisher component unspecified Vulnerability (apr-2009/CVE-2009-0990)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server "BI Publisher" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>
- * CERT: TA09-105A
<http://www.us-cert.gov/cas/techalerts/TA09-105A.html>
- * OSVDB: 53743
<http://osvdb.org/53743>
- * SECTRACK: 1022055
<http://www.securitytracker.com/id?1022055>
- * SECUNIA: 34693
<http://secunia.com/advisories/34693>

CVE Reference:

CVE-2009-0990 (cve.mitre.org, nvd.nist.gov)

• **18368 Oracle Application Server - Outside In Technology component unspecified Vulnerability (apr-2009/CVE-2009-1008)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Outside In Technology" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>
- * CERT: TA09-105A
<http://www.us-cert.gov/cas/techalerts/TA09-105A.html>
- * OSVDB: 53747
<http://osvdb.org/53747>
- * SECTRACK: 1022055
<http://www.securitytracker.com/id?1022055>

* SECUNIA: 34693

<http://secunia.com/advisories/34693>

CVE Reference:

CVE-2009-1008 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-0720 HP CVSS 2.0 Score = 10.0

Unspecified vulnerability in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to execute arbitrary code via unknown vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=124146030732511&w=2>

HP: <http://marc.info/?l=bugtraq&m=124146030732511&w=2>

VUPEN: <http://www.vupen.com/english/advisories/2009/1250>

SECTRAK: <http://www.securitytracker.com/id?1022163>

SECUNIA: <http://secunia.com/advisories/34942>

OSVDB: <http://osvdb.org/54222>

CVE Reference: [CVE-2009-0720](http://cve.mitre.org/cve/2009/0720)

• CVE-2009-1490 Sendmail CVSS 2.0 Score = 5.0

Heap-based buffer overflow in Sendmail before 8.13.2 allows remote attackers to cause a denial of service (daemon crash) and possibly execute arbitrary code via a long X- header, as demonstrated by an X-Testing header.

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

References:

CONFIRM: <http://www.sendmail.org/releases/8.13.2>

XF: <http://xforce.iss.net/xforce/xfdb/50355>

MISC: <http://www.nmrc.org/~thegnome/blog/apr09/>

CVE Reference: [CVE-2009-1490](http://cve.mitre.org/cve/2009/1490)

• CVE-2008-4828 IBM CVSS 2.0 Score = 10.0

Multiple stack-based buffer overflows in dsmagent.exe in the Remote Agent Service in the IBM Tivoli Storage Manager (TSM) client 5.1.0.0 through 5.1.8.2, 5.2.0.0 through 5.2.5.3, 5.3.0.0 through 5.3.6.4, and 5.4.0.0 through 5.4.1.96, and the TSM Express client 5.3.3.0 through 5.3.6.4, allow remote attackers to execute arbitrary code via (1) a request packet that is not properly parsed by an unspecified "generic string handling function" or (2) a crafted nodeName in a dicuGetIdentifyRequest request packet, related to the (a) Web GUI and (b) Java GUI.

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

References:

AIXAPAR: <http://www-1.ibm.com/support/docview.wss?uid=swg1IC59513>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21384389>

VUPEN: <http://www.vupen.com/english/advisories/2009/1235>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/503182/100/0/threaded>

MISC: http://secunia.com/secunia_research/2008-55/

SECUNIA: <http://secunia.com/advisories/32604>

OSVDB: <http://osvdb.org/54232>

OSVDB: <http://osvdb.org/54231>

CVE Reference: [CVE-2008-4828](#)

• **CVE-2009-1520 IBM CVSS 2.0 Score = 10.0**

Buffer overflow in the Web GUI in the IBM Tivoli Storage Manager (TSM) client 5.1.0.0 through 5.1.8.2, 5.2.0.0 through 5.2.5.3, 5.3.0.0 through 5.3.6.4, 5.4.0.0 through 5.4.2.6, and 5.5.0.0 through 5.5.1.17 allows attackers to cause a denial of service (application crash) or execute arbitrary code via unspecified vectors.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/50328>

VUPEN: <http://www.vupen.com/english/advisories/2009/1235>

AIXAPAR: <http://www-1.ibm.com/support/docview.wss?uid=swg1IC59994>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21384389>

SECUNIA: <http://secunia.com/advisories/32604>

CVE Reference: [CVE-2009-1520](#)

• **CVE-2009-1521 IBM CVSS 2.0 Score = 7.5**

Unspecified vulnerability in the Java GUI in the IBM Tivoli Storage Manager (TSM) client 5.2.0.0 through 5.2.5.3, 5.3.0.0 through 5.3.6.5, 5.4.0.0 through 5.4.2.6, and 5.5.0.0 through 5.5.1.17, and the TSM Express client 5.3.3.0 through 5.3.6.5, allows attackers to read or modify arbitrary files via unknown vectors.

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

References:

AIXAPAR: <http://www-1.ibm.com/support/docview.wss?uid=swg1IC59779>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21384389>

XF: <http://xforce.iss.net/xforce/xfdb/50329>

VUPEN: <http://www.vupen.com/english/advisories/2009/1235>

SECUNIA: <http://secunia.com/advisories/32604>

CVE Reference: [CVE-2009-1521](#)

• **CVE-2009-1522 IBM CVSS 2.0 Score = 7.1**

The IBM Tivoli Storage Manager (TSM) client 5.5.0.0 through 5.5.1.17 on AIX and Windows, when SSL is used, allows remote attackers to conduct unspecified man-in-the-middle attacks and read arbitrary files via unknown vectors.

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

References:

AIXAPAR: <http://www-1.ibm.com/support/docview.wss?uid=swg1IC59781>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21384389>

VUPEN: <http://www.vupen.com/english/advisories/2009/1235>

SECUNIA: <http://secunia.com/advisories/32604>

CVE Reference: [CVE-2009-1522](#)

• **CVE-2009-1558 Cisco CVSS 2.0 Score = 7.8**

Directory traversal vulnerability in adm/file.cgi on the Cisco Linksys WVC54GCA wireless video camera with firmware 1.00R22 and 1.00R24 allows remote attackers to read arbitrary files via a %2e. (encoded dot dot) or an absolute pathname in the next_file parameter.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/50231>

VUPEN: <http://www.vupen.com/english/advisories/2009/1173>

BID: <http://www.securityfocus.com/bid/34713>

MISC: <http://www.gnucitizen.org/blog/hacking-linksys-ip-cameras-pt-3/>

CVE Reference: [CVE-2009-1558](#)

• **CVE-2009-1559 Cisco CVSS 2.0 Score = 7.8**

Absolute path traversal vulnerability in adm/file.cgi on the Cisco Linksys WVC54GCA wireless video camera with firmware 1.00R24 and possibly 1.00R22 allows remote attackers to read arbitrary files via an absolute pathname in the this_file parameter. NOTE: traversal via a .. (dot dot) is probably also possible.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/50231>

VUPEN: <http://www.vupen.com/english/advisories/2009/1173>

BID: <http://www.securityfocus.com/bid/34713>

MISC: <http://www.gnucitizen.org/blog/hacking-linksys-ip-cameras-pt-3/>

CVE Reference: [CVE-2009-1559](#)

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