

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

[Sapphire Worm Scanner](#) - The S4 Sapphire 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 Microsoft SQL buffer overflow vulnerability (MS02-039/MS02-061) that the recent Sapphire Worm uses to propagate.

Download Here:

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

This Week in Review

A look at 2008 and cyber crime. SC World Congress to look at best practices. Experts urge Obama to look at cyber security. What does data protection protect?

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

• 2008: A year of cybercriminal innovation

With the emergence of new attack techniques and the reinvention of old ones, 2008 has been a year of cybercriminal innovation.

That's the word according to the "MessageLabs Intelligence: 2008 Annual Security Report," released by Symantec on Thursday.

Among the findings: Malware distribution via social networking sites became more widespread and cybercriminals developed more sophisticated botnets, new ways to launch spam and launched more targeted enterprise attacks.

SC Magazine

Full Story :

<http://www.scmagazineus.com/2008-A-year-of-cybercriminal-innovation/article/122014/>

- **Best practices for companies that have suffered a breach offered at SC World Congress**

What happens after a company suffers a data breach? There are strategies to take to lessen the damage, and to soothe customers whose personal information may now be at risk. And to stay out of the newspapers.

At next week's SC World Congress, experts will be on hand to offer techniques, strategies and procedures companies that have suffered a breach can take to lessen or minimize the damage.

Sometimes, it's not even clear when a company has been put in jeopardy.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Best-practices-for-companies-that-have-suffered-a-breach-offered-at-SC-World-Cong>

- **5 must-do cybersecurity steps for Obama**

December 3, 2008 (CSO) As President-Elect Barack Obama looks for ways to deal with a shattered economy and an ongoing war on terrorism, security experts are urging him to pay attention to something that has a big impact on both: The nation's growing -- and fragile -- cyberinfrastructure.

Meanwhile, retailers increasingly dependent on the Web for commerce have launched online transaction portals that rely on Web applications that are easily targeted by digital miscreants. Many of those features are increasingly accessible via popular social networking sites like Facebook.

With that in mind, CSOnline has compiled a five-point list of areas Obama should focus on, based on feedback from security pros.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9122481&source=rss_topic1

- **Opinion: Is there a hidden cost to data protection?**

December 2, 2008 (Network World) Companies today realize the threats and consequences of data loss and by now most have some sort of data protection in place. But, many companies that were rushed into data protection by the fear of losing precious data may have been too quick to throw together a patchwork quilt of security software, which is now proving costly.

Now that technologies are in place, companies are faced with ongoing auditing and the need to prove to auditors that 1) they did enough to protect themselves and 2) they chose the right paths of protection. In fact, despite implementing a slew of security solutions, companies are finding that they may have not done much to actually lower their risk because they didn't actually understand what data needed to be protected in the first place. Furthermore, the mishmash of security solutions is impossible to manage and have greatly increased costs.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9122102&source=rss_topic1

New Vulnerabilities Tested in SecureScout

- **11029 Cisco IOS EIGRP Network Denial of Service Vulnerability**

EIGRP is an extension protocol of IGRP, a routing protocol used to propagate routing information in internal network environments.

The EIGRP implementation in all versions of IOS is vulnerable to a denial of service if it receives a flood of neighbor announcements.

The issue affects Cisco devices running Cisco Internetwork Operating System Software (IOS) versions 11.3, 12.0(19), 12.1, and 12.2.

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

References:

* BUGTRAQ: 20021219 Cisco IOS EIGRP Network DoS
<http://www.securityfocus.com/archive/1/304034>

* BUGTRAQ: 20021219 Re: Cisco IOS EIGRP Network DoS
<http://www.securityfocus.com/archive/1/304044>
* CISCO: 20021220 Cisco's Response to the EIGRP Issue
http://www.cisco.com/en/US/tech/tk365/technologies_security_notice09186a008011c5e1.html
* FULLDISC: 20051219 Unauthenticated EIGRP DoS
<http://lists.grok.org.uk/pipermail/full-disclosure/2005-December/040330.html>
* FULLDISC: 20051220 RE: Authenticated EIGRP DoS / Information leak
<http://marc.theaimsgroup.com/?l=full-disclosure&m=113504451523186&w=2>
* BUGTRAQ: 20051220 Re: Unauthenticated EIGRP DoS
<http://www.securityfocus.com/archive/1/archive/1/419898/100/0/threaded>
* CONFIRM:
http://www.cisco.com/warp/public/707/eigrp_issue.pdf
* BID: 6443
<http://www.securityfocus.com/bid/6443>
* OSVDB: 18055
<http://www.osvdb.org/18055>
* SECTrack: 1005840
<http://securitytracker.com/id?1005840>
* SECUNIA: 7766
<http://secunia.com/advisories/7766>
* XF: cisco-ios-eigrp-dos(10903)
<http://xforce.iss.net/xforce/xfdb/10903>

CVE Reference:

CVE-2002-2208 (cve.mitre.org, nvd.nist.gov)

• 12131 Cisco Security Advisory: Vulnerability in Cisco IOS Embedded Call Processing Solutions (cisco-sa-20050119-itscme)

ITS, CME and SRST are features that allow a Cisco device running IOS to control IP Phones using the Skinny Call Control Protocol (SCCP). SCCP is the Cisco CallManager native signaling protocol.

Certain malformed packets sent to the SCCP port on an IOS device configured for ITS, CME or SRST may cause the target device to reload.

Successful exploitation of the vulnerability may result in a device reload. Repeated exploitation could result in a Denial of Service (DoS) attack.

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

References:

* BID: 12307
<http://www.securityfocus.com/bid/12307>
* CISCO: 20050119 Vulnerability in Cisco IOS Embedded Call Processing Solutions
<http://www.cisco.com/warp/public/707/cisco-sa-20050119-itscme.shtml>
* SECTrack: 1012945
<http://securitytracker.com/id?1012945>
* SECUNIA: 13913
<http://secunia.com/advisories/13913>
* XF: cisco-ios-sccp-dos(18956)
<http://xforce.iss.net/xforce/xfdb/18956>

CVE Reference:

CVE-2005-0186 (cve.mitre.org, nvd.nist.gov)

• 12132 Cisco IOS Response to AAA Command Authorization by-pass (cisco-sr-20060125-aaatcl)

A vulnerability exists within Cisco Internetwork Operating System (IOS) Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (Tcl) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

Devices not running AAA command authorization feature, or do not support Tcl functionality are not affected by this vulnerability.

Devices impacted by this vulnerability, will allow users to execute any IOS EXEC command at the users authenticated privilege level from within the Tcl shell mode.

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

References:

- * CISCO: 20060125 Response to AAA Command Authorization by-pass
<http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml>
- * BID: 16383
<http://www.securityfocus.com/bid/16383>
- * FRSIRT: ADV-2006-0337
<http://www.frsirt.com/english/advisories/2006/0337>
- * OSVDB: 34892
<http://www.osvdb.org/34892>
- * SECTrack: 1015543
<http://securitytracker.com/id?1015543>
- * SECUNIA: 18613
<http://secunia.com/advisories/18613>
- * XF: cisco-aaa-tcl-auth-bypass(24308)
<http://xforce.iss.net/xforce/xfdb/24308>
- * OSVDB: 22723
<http://www.osvdb.org/22723>

CVE Reference:

- CVE-2006-0485 (cve.mitre.org, nvd.nist.gov)
- CVE-2006-0486 (cve.mitre.org, nvd.nist.gov)

• 13668 Oracle Database Server - Oracle Data Mining component unspecified Vulnerability (oct-2008/CVE-2008-3989)

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

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html>
- * FRSIRT: ADV-2008-2825
<http://www.frsirt.com/english/advisories/2008/2825>
- * SECTrack: 1021050
<http://www.securitytracker.com/id?1021050>
- * SECUNIA: 32291
<http://secunia.com/advisories/32291>

CVE Reference:

- CVE-2008-3989 (cve.mitre.org, nvd.nist.gov)

• 13669 Oracle Database Server - Oracle OLAP component unspecified Vulnerability (oct-2008/CVE-2008-2624)

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

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html>
- * FRSIRT: ADV-2008-2825
<http://www.frsirt.com/english/advisories/2008/2825>
- * SECTrack: 1021050
<http://www.securitytracker.com/id?1021050>
- * SECUNIA: 32291
<http://secunia.com/advisories/32291>
- * XF: oracle-db-olap-unauth-access(45879)
<http://xforce.iss.net/xforce/xfdb/45879>

CVE Reference:

- CVE-2008-2624 (cve.mitre.org, nvd.nist.gov)

• 13670 Oracle Database Server - Change Data Capture component unspecified Vulnerability (oct-2008/CVE-2008-3995)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Change Data Capture" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html>
- * FRSIRT: ADV-2008-2825
<http://www.frsirt.com/english/advisories/2008/2825>
- * SECTrack: 1021050
<http://www.securitytracker.com/id?1021050>
- * SECUNIA: 32291
<http://secunia.com/advisories/32291>

CVE Reference:

CVE-2008-3995 (cve.mitre.org, nvd.nist.gov)

• **13671 Oracle Database Server - Change Data Capture component unspecified Vulnerability (oct-2008/CVE-2008-3996)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Change Data Capture" component.

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html>
- * FRSIRT: ADV-2008-2825
<http://www.frsirt.com/english/advisories/2008/2825>
- * SECUNIA: 32291
<http://secunia.com/advisories/32291>

CVE Reference:

CVE-2008-3996 (cve.mitre.org, nvd.nist.gov)

• **13672 Oracle Database Server - Oracle Data Mining component unspecified Vulnerability (oct-2008/CVE-2008-3992)**

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

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

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2008.html>
- * FRSIRT: ADV-2008-2825
<http://www.frsirt.com/english/advisories/2008/2825>
- * SECUNIA: 32291
<http://secunia.com/advisories/32291>

CVE Reference:

CVE-2008-3992 (cve.mitre.org, nvd.nist.gov)

• **13673 Oracle Database Server - Oracle Spatial component unspecified Vulnerability (oct-2008/CVE-2008-3976)**

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/cpuoct2008.html>
- * FRSIRT: ADV-2008-2825
<http://www.frsirt.com/english/advisories/2008/2825>
- * SECTrack: 1021050
<http://www.securitytracker.com/id?1021050>
- * SECUNIA: 32291
<http://secunia.com/advisories/32291>

CVE Reference:

CVE-2008-3976 (cve.mitre.org, nvd.nist.gov)

• 13674 Oracle Database Server - Workspace Manager component unspecified Vulnerability (oct-2008/CVE-2008-3982)

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/cpuoct2008.html>
- * FRSIRT: ADV-2008-2825 <http://www.frsirt.com/english/advisories/2008/2825>
- * SECTRAK: 1021050 <http://www.securitytracker.com/id?1021050>
- * SECUNIA: 32291 <http://secunia.com/advisories/32291>

CVE Reference:

CVE-2008-3982 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2008-5315 Apple CVSS 2.0 Score = 7.8

Directory traversal vulnerability in the web interface in Apple iPhone Configuration Web Utility 1.0 on Windows allows remote attackers to read arbitrary files via unspecified vectors.

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

References:

- BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/498559/100/0/threaded>
- SECUNIA: <http://secunia.com/advisories/32852>
- FULLDISC: <http://lists.grok.org.uk/pipermail/full-disclosure/2008-November/065822.html>

CVE Reference: [CVE-2008-5315](#)

• CVE-2008-5286 Apple CVSS 2.0 Score = 7.5

Integer overflow in the _cupsImageReadPNG function in CUPS 1.1.17 through 1.3.9 allows remote attackers to execute arbitrary code via a PNG image with a large height value, which bypasses a validation check and triggers a buffer overflow.

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

References:

- BID: <http://www.securityfocus.com/bid/32518>
- CONFIRM: <http://www.cups.org/str.php?L2974>
- MLIST: <http://www.openwall.com/lists/oss-security/2008/12/01/1>
- CONFIRM: <http://svn.easysw.com/public/cups/trunk/CHANGES-1.3.txt>

CVE Reference: [CVE-2008-5286](#)

• CVE-2008-5300 Linux CVSS 2.0 Score = 4.9

Linux kernel 2.6.28 allows local users to cause a denial of service ("soft lockup" and process loss) via a large number of sendmsg function calls, which does not block during AF_UNIX garbage collection and triggers an OOM condition, a different vulnerability than CVE-2008-5029.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=470201

MLIST: <http://marc.info/?l=linux-netdev&m=122765505415944&w=2>

MLIST: <http://marc.info/?l=linux-netdev&m=122721862313564&w=2>

CVE Reference: [CVE-2008-5300](#)

• **CVE-2008-5312 Debian CVSS 2.0 Score = 6.9**

mailscanner 4.55.10 might allow local users to overwrite arbitrary files via a symlink attack on certain temporary files used by the (1) f-prot-autoupdate, (2) clamav-autoupdate, (3) panda-autoupdate.new, (4) trend-autoupdate.new, and (5) rav-autoupdate.new scripts in /etc/MailScanner/autoupdate/, a different vulnerability than CVE-2008-5140.

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

References:

MLIST: <http://www.openwall.com/lists/oss-security/2008/11/29/1>

MISC: <http://bugs.debian.org/506353>

CVE Reference: [CVE-2008-5312](#)

• **CVE-2008-5313 Debian CVSS 2.0 Score = 6.9**

mailscanner 4.68.8 might allow local users to overwrite arbitrary files via a symlink attack on certain temporary files used by the (1) f-prot-autoupdate, (2) clamav-autoupdate, (3) avast-autoupdate, and (4) f-prot-6-autoupdate scripts in /etc/MailScanner/autoupdate/; the (5) bitdefender-wrapper, (6) kaspersky-wrapper, (7) clamav-wrapper, and (8) rav-wrapper scripts in /etc/MailScanner/wrapper/; the (9) Quarantine.pm, (10) TNEF.pm, (11) MessageBatch.pm, (12) WorkArea.pm, and (13) SA.pm scripts in /usr/share/MailScanner/MailScanner/; (14) /usr/sbin/MailScanner; and (15) scripts that load the /etc/MailScanner/mailscanner.conf.with.mcp configuration file.

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

References:

MLIST: <http://www.openwall.com/lists/oss-security/2008/11/29/1>

MISC: <http://bugs.debian.org/506353>

CVE Reference: [CVE-2008-5313](#)

• **CVE-2008-4314 Samba CVSS 2.0 Score = 8.5**

smbd in Samba 3.0.29 through 3.2.4 might allow remote attackers to read arbitrary memory and cause a denial of service via crafted (1) trans, (2) trans2, and (3) ntrans requests, related to a "cut&paste error" that causes an improper bounds check to be performed.

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

References:

UBUNTU: <http://www.ubuntu.com/usn/USN-680-1>

SECTRAK: <http://www.securitytracker.com/id?1021287>

BID: <http://www.securityfocus.com/bid/32494>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/3277>

CONFIRM: <http://us1.samba.org/samba/security/CVE-2008-4314.html>

CONFIRM: <http://us1.samba.org/samba/ftp/patches/security/samba-3.0.32-CVE-2008-4314.patch>

SECUNIA: <http://secunia.com/advisories/32919>

SECUNIA: <http://secunia.com/advisories/32813>

OSVDB: <http://osvdb.org/50230>

CVE Reference: [CVE-2008-4314](#)

• **CVE-2008-5285 Wireshark CVSS 2.0 Score = 5.0**

Wireshark 1.0.4 and earlier allows remote attackers to cause a denial of service via a long SMTP request, which triggers an infinite loop.

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

References:

SECUNIA: <http://secunia.com/advisories/32840>

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=472737

SECTRAK: <http://www.securitytracker.com/id?1021275>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/498562/100/0/threaded>

MLIST: <http://www.openwall.com/lists/oss-security/2008/11/24/1>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/3231>

FULLDISC: <http://lists.grok.org.uk/pipermail/full-disclosure/2008-November/065840.html>

CVE Reference: [CVE-2008-5285](https://cve.mitre.org/cgi-bin/cvequery/search.xml?query=CVE-2008-5285)

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