netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 30

July 25, 2008

Table of Contents

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.

This Week in Review

US-CERT advisory on dns vulnerability. The North American Electric Reliability Corporation to improve grid reliability. A story from real life. Beware of the angry employee.

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

- **22 Jul 2008 15:39:50 DNS flaw details heighten urgency to patch**

Updated Tuesday, July 22 at 5:11 p.m. EST

A researcher has publicly exposed details surrounding a major design vulnerability in the domain name system (DNS) protocol, rejecting a request by the flaw"s discoverer

to avoid speculation.

As a result of the vulnerability details - later confirmed by a research firm that had been briefed on the issue by the bug"s discover, Dan Kaminsky - US-CERT issued an advisory urging businesses to patch their DNS name servers immediately. Experts believe attack code is not far off.

SC Magazine

Full story:

http://feeds.feedburner.com/~r/SCMagazineNews/~3/342853076/

- **21 Jul 2008 15:56:43 NERC unveils cybersecurity plan**

A new response plan for threats to the national power grid is in the works.

The North American Electric Reliability Corporation (NERC), has announced plans for improving grid reliability by enabling faster and more effective action to protect critical assets from cyber or physical threats.

"Cybersecurity is a critical component of grid reliability, but is, by its nature, fundamentally different from any other reliability concern we currently address through our standards, analysis, or enforcement programs," said NERC"s president and chief executive officer, Rick Sergel, in a statement. "It therefore requires a different approach; one that allows for more expedient treatment of critical information, urgent action on standards, and more thorough threat analysis and risk assessment."

SC Magazine

Full story:

http://feeds.feedburner.com/~r/SCMagazineNews/~3/341884079/

- **21 Jul 2008 13:00:00 For Once, Some Incontestable ROI**

July 21, 2008 (Computerworld) Return on investment can be tough to calculate in the realm of information security. Usually, you can"t do much more than point to some "soft" ROI, such as an improved security posture for the company or the marketing advantage of being able to tout how secure your products are.

The investment in this case was our data leak prevention infrastructure, which we rely

on for detecting attempts to send any of our intellectual property out of the company. For a while, the technology was hit-or-miss for us; as with any intrusion-detection software, this technology is prone to false positives until it"s tuned properly. That can result in the "boy who cried wolf" syndrome.

ACTION PLAN: Leverage the incident for more security investments.

Computerworld

Full story:
http://feeds.computerworld.com/~r/Computerworld/Security/News/~3/341182877/article.do

- **21 Jul 2008 13:00:00 Who Pays?**

July 21, 2008 (Computerworld) What do you do when a network administrator goes bad? That"s the question IT staffers for the city of San Francisco are facing this week. One of their own, a net admin named Terry Childs, was arrested for sabotaging the city government"s new fiber backbone network (see story).

Until recently, Childs was well regarded in his IT shop. But last month, that all began to unravel. On June 20, Childs reportedly went after the IT department"s newly hired head of security, chasing her with a camera until she locked herself in an office to escape.

Computerworld

Full story:
http://feeds.computerworld.com/~r/Computerworld/Security/News/~3/341182883/article.do

New Vulnerabilities Tested in SecureScout

- **12157 OpenSSH "X11UseLocalhost" X11 Forwarding Security Issue**

When attempting to bind(2) to a port that has previously been bound with SO_REUSEADDR set, most operating systems check that either the effective user-id matches the previous bind (common on BSD-derived systems) or that the bind addresses do not overlap (Linux and Solaris).

Some operating systems, such as HP/UX, do not perform these checks and are vulnerable to an X11 man-in-the-middle attack when the sshd_config(5) option X11UseLocalhost has been set to "no" - an attacker may establish a more-specific bind, which will be used in preference to sshd's wildcard listener.

Modern BSD operating systems, Linux, OS X and Solaris implement the above checks and are not vulnerable to this attack, nor are systems where the X11UseLocalhost has been left at the default value of "yes".

Portable OpenSSH 5.1 avoids this problem for all operating systems by not setting SO_REUSEADDR when X11UseLocalhost is set to no.

The issue has been reported in versions 5.x prior to 5.1 and 5.1p1.

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

References:

* FRSIRT: FrSIRT/ADV-2008-2148

http://www.frsirt.com/english/advisories/2008/2148

* BID: 30339

http://www.securityfocus.com/bid/30339

* MISC: OpenSSH 5.1 Release Notes

http://www.openssh.com/txt/release-5.1

* SECUNIA: 31179

http://secunia.com/advisories/31179/

CVE Reference:

• 13656 Oracle Database Server - Instance Management component unspecified Vulnerability (jul-2008/CVE-2008-2590)

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

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

References:

* SECUNIA: 31087

http://secunia.com/advisories/31087/

* CONFIRM:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference:

CVE-2008-2590 (cve.mitre.org, nvd.nist.gov)

- **13657 Oracle Database Server - Resource Manager component unspecified Vulnerability (jul-2008/CVE-2008-2603)**

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

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

References:

* SECUNIA: 31087

http://secunia.com/advisories/31087/

* CONFIRM:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference:

CVE-2008-2603 (cve.mitre.org, nvd.nist.gov)

- **13658 Oracle Database Server - Advanced Replication component unspecified Vulnerability (jul-2008/CVE-2008-2587)**

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

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

References:

* SECUNIA: 31087

http://secunia.com/advisories/31087/

* CONFIRM:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference:

CVE-2008-2587 (cve.mitre.org, nvd.nist.gov)

- **16982 Windows Saved Search Vulnerability (MS08-038/950582) (Remote File Checking)**

A remote code execution vulnerability exists when saving a specially crafted search file within Windows Explorer. This operation causes Windows Explorer to exit and restart in an exploitable manner.

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

References:

* MS: MS08-038

http://www.microsoft.com/technet/security/bulletin/ms08-038.mspx

* SECTRACK: 1020436

http://www.securitytracker.com/id?1020436

* SECUNIA: 30953

http://secunia.com/advisories/30953

* FRSIRT: FrSIRT/ADV-2008-2020

http://www.frsirt.com/english/advisories/2008/2020

* SECTRACK: 1020436

http://securitytracker.com/alerts/2008/Jul/1020436.html

* BID: 30109

http://www.securityfocus.com/bid/30109

CVE Reference:

CVE-2008-1435 (cve.mitre.org, nvd.nist.gov)

- **17703 Apache, Error page XSS using wildcard DNS**

Cross-site scripting (XSS) vulnerability in the default error page of Apache 2.0 before 2.0.43, and 1.3.x up to 1.3.26, when UseCanonicalName is "Off" and support for wildcard DNS is present, allows remote attackers to execute script as other web page

visitors via the Host: header.

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

References:

BUGTRAQ: 20021002 Apache 2 Cross-Site Scripting

http://marc.theaimsgroup.com/?l=bugtraq&m=103357160425708&w=2

* VULNWATCH: 20021002 Apache 2 Cross-Site Scripting

http://archives.neohapsis.com/archives/vulnwatch/2002-q4/0003.html

* CONFIRM:

http://www.apacheweek.com/issues/02-10-04

* CONFIRM:

http://marc.theaimsgroup.com/?l=apache-httpd-announce&m=103367938230488&w=2

* DEBIAN: DSA-187

http://www.debian.org/security/2002/dsa-187

* DEBIAN: DSA-188

http://www.debian.org/security/2002/dsa-188

* DEBIAN: DSA-195

http://www.debian.org/security/2002/dsa-195

* HP: HPSBUX0210-224

http://online.securityfocus.com/advisories/4617

* BUGTRAQ: 20021003 [OpenPKG-SA-2002.009] OpenPKG Security Advisory (apache)

http://marc.theaimsgroup.com/?l=bugtraq&m=103376585508776&w=2

* BUGTRAQ: 20021017 TSLSA-2002-0069-apache

http://archives.neohapsis.com/archives/bugtraq/2002-10/0254.html

* REDHAT: RHSA-2002:222

http://www.redhat.com/support/errata/RHSA-2002-222.html

* REDHAT: RHSA-2002:243

http://www.redhat.com/support/errata/RHSA-2002-243.html

* REDHAT: RHSA-2002:244

http://www.redhat.com/support/errata/RHSA-2002-244.html

* REDHAT: RHSA-2002:248

http://www.redhat.com/support/errata/RHSA-2002-248.html

* REDHAT: RHSA-2002:251

http://www.redhat.com/support/errata/RHSA-2002-251.html

* REDHAT: RHSA-2003:106

http://www.redhat.com/support/errata/RHSA-2003-106.html

* SGI: 20021105-02-I

ftp://patches.sgi.com/support/free/security/advisories/20021105-02-I

* CERT-VN: VU#240329

http://www.kb.cert.org/vuls/id/240329

* XF: apache-http-host-xss(10241)

http://xforce.iss.net/xforce/xfdb/10241

* BID: 5847

http://www.securityfocus.com/bid/5847

* OSVDB: 862

http://www.osvdb.org/862

CVE Reference:

CVE-2002-0840 (cve.mitre.org, nvd.nist.gov)

- **13652 Apache, Shared memory permissions lead to local privilege escalation**

The permissions of the shared memory used for the scoreboard allow an attacker who can execute under the Apache UID to send a signal to any process as root or cause a local denial of service attack.

The vulnerability has been reported in Apache 1.3.x up to 1.3.26.

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

References:

* VULNWATCH: 20021003 iDEFENSE Security Advisory 10.03.2002: Apache 1.3.x shared memory scoreboard vulnerabilities

http://archives.neohapsis.com/archives/vulnwatch/2002-q4/0012.html

* CONFIRM:

http://www.apacheweek.com/issues/02-10-04

* CONFIRM:

http://marc.theaimsgroup.com/?l=apache-httpd-announce&m=103367938230488&w=2

* DEBIAN: DSA-187

http://www.debian.org/security/2002/dsa-187

* DEBIAN: DSA-188

http://www.debian.org/security/2002/dsa-188

* DEBIAN: DSA-195

http://www.debian.org/security/2002/dsa-195

* BUGTRAQ: 20021003 [OpenPKG-SA-2002.009] OpenPKG Security Advisory (apache)

http://marc.theaimsgroup.com/?l=bugtraq&m=103376585508776&w=2

* SGI: 20021105-01-I

ftp://patches.sgi.com/support/free/security/advisories/20021105-01-I

* HP: HPSBUX0210-224

http://online.securityfocus.com/advisories/4617

* BUGTRAQ: 20021015 GLSA: apache

http://archives.neohapsis.com/archives/bugtraq/2002-10/0195.html

* BUGTRAQ: 20021017 TSLSA-2002-0069-apache

http://archives.neohapsis.com/archives/bugtraq/2002-10/0254.html

* BID: 5884

http://www.securityfocus.com/bid/5884

* XF: apache-scorecard-memory-overwrite(10280)

http://www.iss.net/security_center/static/10280.php

CVE Reference:

CVE-2002-0839 (cve.mitre.org, nvd.nist.gov)

- **17798 Apache, Buffer overflows in ab utility**

Buffer overflows in the benchmarking utility ab could be exploited if ab is run against a malicious server

The vulnerabilities have been reported in Apache 1.3.x up to 1.3.26.

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

References:

* BUGTRAQ: 20021016 Apache 1.3.26

http://archives.neohapsis.com/archives/bugtraq/2002-10/0229.html

* CONFIRM:

http://www.apacheweek.com/issues/02-10-04

* CONFIRM:

http://marc.theaimsgroup.com/?l=apache-httpd-announce&m=103367938230488&w=2

* CONFIRM:

http://www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd?mode=18&ID=2871

* AIXAPAR: IY87070

http://www-1.ibm.com/support/search.wss?rs=0&q=IY87070&apar=only

* DEBIAN: DSA-187

http://www.debian.org/security/2002/dsa-187

* DEBIAN: DSA-188

http://www.debian.org/security/2002/dsa-188

* DEBIAN: DSA-195

http://www.debian.org/security/2002/dsa-195

* HP: HPSBUX0210-224

http://online.securityfocus.com/advisories/4617

* SGI: 20021105-01-I

ftp://patches.sgi.com/support/free/security/advisories/20021105-01-I

* BUGTRAQ: 20021003 [OpenPKG-SA-2002.009] OpenPKG Security Advisory (apache)

http://marc.theaimsgroup.com/?l=bugtraq&m=103376585508776&w=2

* BUGTRAQ: 20021017 TSLSA-2002-0069-apache

http://archives.neohapsis.com/archives/bugtraq/2002-10/0254.html

* BID: 5995

http://www.securityfocus.com/bid/5995

* BID: 5996

http://www.securityfocus.com/bid/5996

* FRSIRT: ADV-2006-3263

http://www.frsirt.com/english/advisories/2006/3263

* SECUNIA: 21425

http://secunia.com/advisories/21425

* XF: apache-apachebench-response-bo(10281)

http://www.iss.net/security_center/static/10281.php

CVE Reference:

CVE-2002-0843 (cve.mitre.org, nvd.nist.gov)

- **17799 Apache, Filtered escape sequences**

Apache did not filter terminal escape sequences from its access logs, which could make it easier for attackers to insert those sequences into terminal emulators containing vulnerabilities related to escape sequences.

The vulnerability has been confirmed in Apache 1.3.x up to 1.3.24 and 2.0.x up to 2.0.45.

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

References:

* REDHAT: RHSA-2003:139

http://www.redhat.com/support/errata/RHSA-2003-139.html

* BUGTRAQ: 20040325 GLSA200403-04 Multiple security vulnerabilities in Apache 2

http://marc.theaimsgroup.com/?l=bugtraq&m=108024081011678&w=2

* BUGTRAQ: 20040325 LNSA-#2004-0006: bug workaround for Apache 2.0.48

http://marc.theaimsgroup.com/?l=bugtraq&m=108034113406858&w=2

* OVAL: oval:org.mitre.oval:def:151

http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:151

* SECUNIA: 8146

http://secunia.com/advisories/8146

CVE Reference:

CVE-2003-0083 (cve.mitre.org, nvd.nist.gov)

- **18028 Apache, Error log escape filtering)**

Apache does not filter terminal escape sequences from error logs, which could make it easier for attackers to insert those sequences into terminal emulators containing vulnerabilities related to escape sequences.

The vulnerability has been confirmed in Apache 1.3.x up to 1.3.29 and 2.0.x up to 2.0.48.

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

References:

* VULNWATCH: 20030224 Terminal Emulator Security Issues

http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0093.html

* BUGTRAQ: 20030224 Terminal Emulator Security Issues

http://marc.theaimsgroup.com/?l=bugtraq&m=104612710031920&w=2

* APPLE: APPLE-SA-2004-05-03

http://marc.theaimsgroup.com/?l=bugtraq&m=108369640424244&w=2

* HP: SSRT4717

http://marc.theaimsgroup.com/?l=bugtraq&m=108731648532365&w=2

* MANDRAKE: MDKSA-2004:046

http://frontal2.mandriva.com/security/advisories?name=MDKSA-2004:046

* REDHAT: RHSA-2003:082

http://www.redhat.com/support/errata/RHSA-2003-082.html

* REDHAT: RHSA-2003:083

http://www.redhat.com/support/errata/RHSA-2003-083.html

* REDHAT: RHSA-2003:104

http://www.redhat.com/support/errata/RHSA-2003-104.html

* REDHAT: RHSA-2003:139

http://www.redhat.com/support/errata/RHSA-2003-139.html

* REDHAT: RHSA-2003:243

http://www.redhat.com/support/errata/RHSA-2003-243.html

* REDHAT: RHSA-2003:244

http://www.redhat.com/support/errata/RHSA-2003-244.html

* SLACKWARE: SSA:2004-133

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.529643

* SUNALERT: 57628

http://sunsolve.sun.com/search/document.do?assetkey=1-26-57628-1

* SUNALERT: 101555

http://sunsolve.sun.com/search/document.do?assetkey=1-26-101555-1

* TRUSTIX: 2004-0017

http://www.trustix.org/errata/2004/0017

* TRUSTIX: 2004-0027

http://www.trustix.org/errata/2004/0027

* BUGTRAQ: 20040512 [OpenPKG-SA-2004.021] OpenPKG Security Advisory (apache)

http://marc.theaimsgroup.com/?l=bugtraq&m=108437852004207&w=2

* XF: apache-esc-seq-injection(11412)

http://www.iss.net/security_center/static/11412.php

* BID: 9930

http://www.securityfocus.com/bid/9930

* OVAL: oval:org.mitre.oval:def:150

http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:150

* OVAL: oval:org.mitre.oval:def:4114

http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4114

* OVAL: oval:org.mitre.oval:def:100109

http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:100109

CVE Reference:

CVE-2003-0020 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2008-3173 Microsoft CVSS 2.0 Score = 6.8**

Microsoft Internet Explorer allows web sites to set cookies for domains that have a public suffix with more than one dot character, which could allow remote attackers to perform a session fixation attack and hijack a user's HTTP session, aka "Cross-Site Cooking." NOTE: this issue may exist because of an insufficient fix for CVE-2004-0866.

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

References:

http://crisp.tweakblogs.net/blog/ie-and-2-letter-domain-names.html

http://kuza55.blogspot.com/2008/02/understanding-cookie-security.html

CVE Reference: CVE-2008-3173

- **CVE-2008-2579 Microsoft CVSS 2.0 Score = 6.8**

Unspecified vulnerability in the WebLogic Server Plugins for Apache, Sun and IIS web servers component in BEA Product Suite 10.0 MP1, 9.2 MP3, 9.1, 9.0, 8.1 SP6, 7.0 SP7, and 6.1 SP7 has unknown impact and remote attack vectors.

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

References:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference: CVE-2008-2579

- **CVE-2008-2597 Oracle CVSS 2.0 Score = 7.5**

Unspecified vulnerability in the TimesTen Client/Server component in Oracle Times Ten In-Memory Database 7.0.3.0.0 has unknown impact and remote attack vectors, a different vulnerability than CVE-2008-2598 and CVE-2008-2599.

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

References:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference: CVE-2008-2597

- **CVE-2008-2598 Oracle CVSS 2.0 Score = 7.5**

Unspecified vulnerability in the TimesTen Client/Server component in Oracle Times Ten In-Memory Database 7.0.3.0.0 has unknown impact and remote attack vectors, a different vulnerability than CVE-2008-2597 and CVE-2008-2599.

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

References:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference: CVE-2008-2598

- **CVE-2008-2599 Oracle CVSS 2.0 Score = 7.5**

Unspecified vulnerability in the TimesTen Client/Server component in Oracle Times Ten In-Memory Database 7.0.3.0.0 has unknown impact and remote attack vectors, a different vulnerability than CVE-2008-2597 and CVE-2008-2598.

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

References:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference: CVE-2008-2599

- **CVE-2008-2609 Oracle CVSS 2.0 Score = 7.5**

Unspecified vulnerability in the Oracle Portal component in Oracle Application Server 9.0.4.3, 10.1.2.3, and 10.1.4.2 has unknown impact and remote attack vectors.

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

References:

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html

CVE Reference: CVE-2008-2609

- **CVE-2008-1666 HP CVSS 2.0 Score = 10.0**

Unspecified vulnerability in HP Oracle for OpenView (OfO) 8.1.7, 9.1.01, 9.2, 9.2.0, 10g, and 10gR2 has unknown impact and attack vectors, possibly related to the July 2008 Oracle Critical Patch Update.

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

References:

HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00727143

FRSIRT: http://www.frsirt.com/english/advisories/2008/2115

SECUNIA: http://secunia.com/advisories/31113

CVE Reference: CVE-2008-1666

- **CVE-2008-1665 HP CVSS 2.0 Score = 9.0**

Multiple unspecified vulnerabilities in HP Select Identity (HPSI) Active Directory Bidirectional LDAP Connector 2.20, 2.20.001, 2.20.002, and 2.30 allow remote attackers to execute arbitrary code via unspecified vectors.

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

References:

HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01502023

CVE Reference: CVE-2008-1665

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