

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

[CodeRed Worm Scanner](#) - The S4 CodeRed Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any have been infected by CodeRed Worm.

Download Here:

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

This Week in Review

Vulnerability management hard to grasp for companies. Privacy or accessibility - take your pick. Expect lower IT budgets, but not for security spendings. Domain registrar in Estonia loses right to register new domains.

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

• IT security policy enforcement struggles

Companies are struggling to come to grips with the basics of vulnerability management, says Chris Schwartzbauer, vice president of development and customer operations at Shavlik Technologies.

"You can't secure what you don't know about, and unfortunately the unknowns are many," Schwartzbauer said. "IT administrators are often unaware of all of the servers live on their network, let alone their relevance or desired configuration, mobile computers are missed during scheduled vulnerability checks, old or unauthorized account privileges persist. And virtualization has made it all too easy for users to 'create' more machines that must be protected."

"Decision makers, the CIO, security and risk managers assume the basics are resolved because the investment has been made in sophisticated security strategy and technologies," he said. "But it is in the mundane processes, the policy and configuration management, where the vulnerability gaps are left wide open."

Full Story :

<http://www.scmagazineus.com/IT-security-policy-enforcement-struggles/article/120161/>

• Opinion: What trumps privacy?

October 30, 2008 (Computerworld) We all like to think our privacy is absolute. But if your job involves working across borders, you'll want to talk about privacy as a matter of degree rather than as an uncompromising right. Why? Not only do you want to be seen as someone who can get things done globally, but you also may personally want to be part of advancing social objectives that are arguably as important as privacy.

It's a popular idea. The half-billion people of Europe do view privacy as a human right. And they're not the only ones. As one of the first acts of the UN, Eleanor Roosevelt and the U.S. delegation in 1948 lobbied for the global adoption of the Universal Declaration of Human Rights(UNDHR), whose Article 12 states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9118600&source=rss_topic1

• IT security spending not darkened by economic gloom

October 28, 2008 (Network World) The global financial crisis, so visible this past month, is beginning to take its toll on IT spending, though IT security spending is expected to be spared in what many think will be a dismal coming year.

Even in the midst of this turmoil, spending on IT security will largely escape the cost-cutting measures anticipated for other aspects of IT. That's an opinion shared by some network managers -- at least for now.

Temple University, which just swapped out an older stand-alone Check Point firewall and IBM ISS Proventia intrusion-prevention system for a single Crossbeam unified threat management device combining both technologies, is not expected to cut back on planned security projects.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9118378&source=rss_topic1

• ICANN cuts ties with Estonia domain registrar

The Internet Corp. for Assigned Names and Numbers (ICANN) has revoked an Estonia-based domain registrar's right to issue any new addresses.

In February, Vladimir Tsastsin, president of EstDomains, was convicted of credit card fraud, money laundering and document forgery, according to a letter (PDF) sent by ICANN to Tsastsin.

Under ICANN rules, the organization can end its accreditation agreement with any registrar whose "officer or director...is convicted of a felony or of a misdemeanor related to financial activities..." the letter said.

SC Magazine

Full Story :

<http://www.scmagazineus.com/ICANN-cuts-ties-with-Estonia-domain-registrar/article/120191/>

New Vulnerabilities Tested in SecureScout

• 12158 OpenSSH Authentication Implementation Error Vulnerability

OpenSSH contains a flaw that may allow a malicious user to successfully authenticate with the password of another user. The issue is triggered when OpenSSH is running on an OpenBSD system using YP and Netgroups for password authentication. It is possible that the flaw may allow incorrectly approved authentication, resulting in a loss of confidentiality.

The vulnerability is reported in versions 3.1 and 3.2.2.

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

References:

* BUGTRAQ: 20020527 OpenSSH 3.2.3 released (fwd)
<http://archives.neohapsis.com/archives/bugtraq/2002-05/0235.html>

* OPENBSD: 20020522 004: SECURITY FIX: May 22, 2002
<http://www.openbsd.org/errata.html#sshbsdauth>
* BID: 4803
<http://www.securityfocus.com/bid/4803>
* XF: bsd-sshd-authentication-error(9215)
http://www.iss.net/security_center/static/9215.php
* OSVDB: 5113
<http://www.osvdb.org/5113>

CVE Reference:

CVE-2002-0765 (cve.mitre.org, nvd.nist.gov)

• 12159 OpenSSH "Memory bugs" Vulnerabilities

OpenSSH 3.7.1 and earlier, is impacted by some "Memory bugs".

The vulnerability has been reported in versions 3.7.1 and prior.

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

References:

* REDHAT: RHSA-2003:279
<http://marc.theaimsgroup.com/?l=bugtraq&m=106373546332230&w=2>
* REDHAT: RHSA-2003:280
<http://www.redhat.com/support/errata/RHSA-2003-280.html>
* DEBIAN: DSA-382
<http://www.debian.org/security/2003/dsa-382>
* DEBIAN: DSA-383
<http://www.debian.org/security/2003/dsa-383>
* BUGTRAQ: 20030917 [OpenPKG-SA-2003.040] OpenPKG Security Advisory (openssh)
<http://marc.theaimsgroup.com/?l=bugtraq&m=106381409220492&w=2>
* OVAL: oval:org.mitre.oval:def:446
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:446>

CVE Reference:

CVE-2003-0682 (cve.mitre.org, nvd.nist.gov)

• 12160 OpenSSH SCP Client File Corruption Vulnerability

Directory traversal vulnerability in scp for OpenSSH before 3.4p1 allows remote malicious servers to overwrite arbitrary files.

The vulnerability is reported in versions prior to 3.4p1.

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

References:

* CONFIRM:
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=120147
* CONFIRM:
<http://www.juniper.net/support/security/alerts/adv59739.txt>
* MANDRIVA: MDKSA-2005:100
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:100>
* MANDRIVA: MDVSA-2008:191
<http://www.mandriva.com/security/advisories?name=MDVSA-2008:191>
* REDHAT: RHSA-2005:106
<http://www.redhat.com/support/errata/RHSA-2005-106.html>
* REDHAT: RHSA-2005:074
<http://www.redhat.com/support/errata/RHSA-2005-074.html>
* REDHAT: RHSA-2005:165
<http://www.redhat.com/support/errata/RHSA-2005-165.html>
* REDHAT: RHSA-2005:481
<http://www.redhat.com/support/errata/RHSA-2005-481.html>
* REDHAT: RHSA-2005:495
<http://www.redhat.com/support/errata/RHSA-2005-495.html>
* REDHAT: RHSA-2005:562
<http://www.redhat.com/support/errata/RHSA-2005-562.html>
* REDHAT: RHSA-2005:567
<http://www.redhat.com/support/errata/RHSA-2005-567.html>

* SCO: SCOSA-2006.11
<ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2006.11/SCOSA-2006.11.txt>
* SUSE: SuSE-SA:2004:009
http://www.novell.com/linux/security/advisories/2004_09_kernel.html
* CIAC: O-212
<http://www.ciac.org/ciac/bulletins/o-212.shtml>
* BID: 9986
<http://www.securityfocus.com/bid/9986>
* OSVDB: 9550
<http://www.osvdb.org/9550>
* SECUNIA: 19243
<http://secunia.com/advisories/19243>
* SECUNIA: 17135
<http://secunia.com/advisories/17135>
* XF: openssh-scp-file-overwrite(16323)
<http://xforce.iss.net/xforce/xfdb/16323>

CVE Reference:

CVE-2004-0175 (cve.mitre.org, nvd.nist.gov)

• 12161 OpenSSH Remote Root Authentication Timing Side-Channel Weakness

sshd in OpenSSH 3.6.1p2 and earlier, when PermitRootLogin is disabled and using PAM keyboard-interactive authentication, does not insert a delay after a root login attempt with the correct password, which makes it easier for remote attackers to use timing differences to determine if the password step of a multi-step authentication is successful.

The vulnerability is reported in versions 3.6.1p2 and earlier.

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

References:

* BUGTRAQ: 20030501 Re: OpenSSH/PAM timing attack allows remote users identification
<http://www.securityfocus.com/archive/1/320153>
* BUGTRAQ: 20030501 Re: OpenSSH/PAM timing attack allows remote users identification
<http://www.securityfocus.com/archive/1/320302>
* BUGTRAQ: 20030505 Re: OpenSSH/PAM timing attack allows remote users identification
<http://www.securityfocus.com/archive/1/320440>
* CONFIRM:
<http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=248747>
* BID: 7482
<http://www.securityfocus.com/bid/7482>

CVE Reference:

CVE-2003-1562 (cve.mitre.org, nvd.nist.gov)

• 12162 OpenSSH LoginGraceTime Remote Denial Of Service Vulnerability

sshd.c in OpenSSH 3.6.1p2 and 3.7.1p2 and possibly other versions, when using privilege separation, does not properly signal the non-privileged process when a session has been terminated after exceeding the LoginGraceTime setting, which leaves the connection open and allows remote attackers to cause a denial of service (connection consumption).

The vulnerability is reported in versions 3.7.1p2 and earlier.

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

References:

* BUGTRAQ: 20061113 VMSA-2006-0006 - VMware ESX Server 2.5.3 Upgrade Patch 4
<http://www.securityfocus.com/archive/1/archive/1/451404/100/0/threaded>
* BUGTRAQ: 20061113 VMSA-2006-0007 - VMware ESX Server 2.1.3 Upgrade Patch 2
<http://www.securityfocus.com/archive/1/archive/1/451417/100/200/threaded>
* BUGTRAQ: 20061113 VMSA-2006-0008 - VMware ESX Server 2.0.2 Upgrade Patch 2
<http://www.securityfocus.com/archive/1/archive/1/451426/100/200/threaded>
* MLIST: [openssh-unix-dev] 20040127 OpenSSH - Connection problem when LoginGraceTime exceeds time
<http://marc.theaimsgroup.com/?l=openssh-unix-dev&m=107520317020444&w=2>
* MLIST: [openssh-unix-dev] 20040128 Re: OpenSSH - Connection problem when LoginGraceTime exceeds time
<http://marc.theaimsgroup.com/?l=openssh-unix-dev&m=107529205602320&w=2>
* CONFIRM:

<http://support.avaya.com/elmodocs2/security/ASA-2005-216.pdf>
* CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2005-223.pdf>
* CONFIRM:
<http://www.vmware.com/download/esx/esx-202-200610-patch.html>
* CONFIRM:
<http://www.vmware.com/download/esx/esx-213-200610-patch.html>
* CONFIRM:
<http://www.vmware.com/support/vi3/doc/esx-3069097-patch.html>
* CONFIRM:
<http://www.vmware.com/support/vi3/doc/esx-9986131-patch.html>
* FEDORA: FLSA-2006:168935
<http://www.securityfocus.com/archive/1/archive/1/425397/100/0/threaded>
* REDHAT: RHSA-2005:550
<http://rhn.redhat.com/errata/RHSA-2005-550.html>
* BID: 14963
<http://www.securityfocus.com/bid/14963>
* FRSIRT: ADV-2006-4502
<http://www.frsirt.com/english/advisories/2006/4502>
* OSVDB: 16567
<http://www.osvdb.org/16567>
* SECUNIA: 17135
<http://secunia.com/advisories/17135>
* SECUNIA: 17252
<http://secunia.com/advisories/17252>
* SECUNIA: 17000
<http://secunia.com/advisories/17000>
* SECUNIA: 22875
<http://secunia.com/advisories/22875>
* SECUNIA: 23680
<http://secunia.com/advisories/23680>
* XF: openssl-sshd-c-logging-race-time-dos(20930)
<http://xforce.iss.net/xforce/xfdb/20930>

CVE Reference:

CVE-2004-2069 (cve.mitre.org, nvd.nist.gov)

• 12163 OpenSSH Address Harvesting Vulnerability

SSH, as implemented in OpenSSH before 4.0 and possibly other implementations, stores hostnames, IP addresses, and keys in plaintext in the known_hosts file, which makes it easier for an attacker that has compromised an SSH user's account to generate a list of additional targets that are more likely to have the same password or key.

The vulnerability is reported in versions prior to 4.0.

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

References:

* MISC:
<http://nms.csail.mit.edu/projects/ssh/>
* MISC:
<http://www.eweek.com/article2/0,1759,1815795,00.asp>
* REDHAT: RHSA-2007:0257
<http://www.redhat.com/support/errata/RHSA-2007-0257.html>
* SCO: SCOSA-2006.11
<ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2006.11/SCOSA-2006.11.txt>
* SECUNIA: 19243
<http://secunia.com/advisories/19243>
* SECUNIA: 25098
<http://secunia.com/advisories/25098>

CVE Reference:

CVE-2005-2666 (cve.mitre.org, nvd.nist.gov)

• 12164 OpenSSH S/Key Remote Information Disclosure Vulnerability

OpenSSH 4.6 and earlier, when ChallengeResponseAuthentication is enabled, allows remote attackers to determine the existence of user accounts by attempting to authenticate via S/KEY, which displays a different response if the user account exists.

The vulnerability is reported in versions 4.6 and earlier.

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

References:

- * FULLDISC: 20070421 OpenSSH - System Account Enumeration if S/Key is used
<http://lists.grok.org.uk/pipermail/full-disclosure/2007-April/053906.html>
- * FULLDISC: 20070424 OpenSSH - System Account Enumeration if S/Key is used
<http://lists.grok.org.uk/pipermail/full-disclosure/2007-April/053951.html>
- * BID: 23601
<http://www.securityfocus.com/bid/23601>
- * OSVDB: 34600
<http://www.osvdb.org/34600>
- * SREASON: 2631
<http://securityreason.com/securityalert/2631>
- * XF: openssh-challenge-information-disclosure(33794)
<http://xforce.iss.net/xforce/xfdb/33794>

CVE Reference:

CVE-2007-2243 (cve.mitre.org, nvd.nist.gov)

• 12165 OpenSSH X11 Cookie Local Authentication Bypass Vulnerability

ssh in OpenSSH before 4.7 does not properly handle when an untrusted cookie cannot be created and uses a trusted X11 cookie instead, which allows attackers to violate intended policy and gain privileges by causing an X client to be treated as trusted.

The vulnerability is reported in versions prior to 4.7.

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

References:

- * BUGTRAQ: 20070917 FLEA-2007-0055-1 openssh openssh-client openssh-server gnome-ssh-askpass
<http://www.securityfocus.com/archive/1/archive/1/479760/100/0/threaded>
- * BUGTRAQ: 20071115 Re: HPSBUX02287 SSRT071485 rev.1 - HP-UX Running HP Secure Shell, Remotely Gain Extended Privileges
<http://www.securityfocus.com/archive/1/archive/1/483748/100/200/threaded>
- * MISC:
https://bugzilla.redhat.com/show_bug.cgi?id=280471
- * CONFIRM:
<http://www.openssh.com/txt/release-4.7>
- * CONFIRM:
<https://issues.rpath.com/browse/RPL-1706>
- * CONFIRM:
http://bugs.gentoo.org/show_bug.cgi?id=191321
- * CONFIRM:
<http://docs.info.apple.com/article.html?artnum=307562>
- * APPLE: APPLE-SA-2008-03-18
<http://lists.apple.com/archives/security-announce/2008/Mar/msg00001.html>
- * DEBIAN: DSA-1576
<http://www.debian.org/security/2008/dsa-1576>
- * FEDORA: FEDORA-2007-715
<https://www.redhat.com/archives/fedora-package-announce/2007-October/msg00214.html>
- * GENTOO: GLSA-200711-02
<http://security.gentoo.org/glsa/glsa-200711-02.xml>
- * HP: HPSBUX02287
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01271085>
- * MANDRIVA: MDKSA-2007:236
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:236>
- * REDHAT: RHSA-2008:0855
<http://www.redhat.com/support/errata/RHSA-2008-0855.html>
- * SUSE: SUSE-SR:2007:022
<http://lists.opensuse.org/opensuse-security-announce/2007-10/msg00008.html>
- * UBUNTU: USN-566-1
<http://www.ubuntu.com/usn/usn-566-1>
- * BID: 25628
<http://www.securityfocus.com/bid/25628>
- * FRSIRT: ADV-2007-3156
<http://www.frsirt.com/english/advisories/2007/3156>

* FRSIRT: ADV-2008-0924
<http://www.frsirt.com/english/advisories/2008/0924/references>
* FRSIRT: ADV-2008-2821
<http://www.frsirt.com/english/advisories/2008/2821>
* SECUNIA: 27399
<http://secunia.com/advisories/27399>
* SECUNIA: 29420
<http://secunia.com/advisories/29420>
* SECUNIA: 30249
<http://secunia.com/advisories/30249>
* SECUNIA: 31575
<http://secunia.com/advisories/31575>
* SREASON: 3126
<http://securityreason.com/securityalert/3126>
* XF: openssh-x11cookie-privilege-escalation(36637)
<http://xforce.iss.net/xforce/xfdb/36637>

CVE Reference:

CVE-2007-4752 (cve.mitre.org, nvd.nist.gov)

• 18183 ProFTPD Long Command Handling Security Vulnerability

ProFTPD is an FTP server available for many Unix platforms.

ProFTPD 1.3.1 interprets long commands from an FTP client as multiple commands, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks and execute arbitrary FTP commands via a long ftp:// URI that leverages an existing session from the FTP client implementation in a web browser.

The issue has been fixed in version 1.3.2.

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

References:

* SREASONRES: 20080926 multiple vendor ftpd - Cross-site request forgery
http://securityreason.com/achievement_securityalert/56
* CONFIRM:
http://bugs.proftpd.org/show_bug.cgi?id=3115
* BID: 31289
<http://www.securityfocus.com/bid/31289>
* SECTRAK: 1020945
<http://www.securitytracker.com/id?1020945>
* SECUNIA: 31930
<http://secunia.com/advisories/31930>
* XF: proftpd-url-csrf(45274)
<http://xforce.iss.net/xforce/xfdb/45274>

CVE Reference:

CVE-2008-4242 (cve.mitre.org, nvd.nist.gov)

• 18184 ProFTPD Mod_Radius Buffer Overflow Vulnerability

ProFTPD is an FTP server available for many Unix platforms.

A buffer overflow in mod_radius in ProFTPD before 1.3.0rc2 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long password.

The issue has been fixed in version 1.3.0rc2.

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

References:

* MLIST: [Dailydave] 20060207 ProFTPD bug
<http://archives.neohapsis.com/archives/dailydave/2006-q1/0122.html>
* CONFIRM:
http://bugs.proftpd.org/show_bug.cgi?id=2658
* DEBIAN: DSA-1245
<http://www.debian.org/security/2007/dsa-1245>
* BID: 16535
<http://www.securityfocus.com/bid/16535>

* OSVDB: 23063

<http://www.osvdb.org/23063>

CVE Reference:

CVE-2005-4816 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2008-4787 Microsoft CVSS 2.0 Score = 5.0

Visual truncation vulnerability in Microsoft Internet Explorer 6 allows remote attackers to spoof the address bar via a URL with a hostname containing many (Non-Blocking Space character) sequences, which are rendered as whitespace, aka MSRC ticket MSRC7899, a related issue to CVE-2003-1025.

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

References:

BID: <http://www.securityfocus.com/bid/31960>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/497827/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/497825/100/0/threaded>

CVE Reference: [CVE-2008-4787](#)

• CVE-2008-4788 Microsoft CVSS 2.0 Score = 5.0

Microsoft Internet Explorer 6 omits high-bit URL-encoded characters when displaying the address bar, which allows remote attackers to spoof the address bar via a URL with a domain name that differs from an important domain name only in these characters, as demonstrated by using exam%A9ple.com to spoof example.com, aka MSRC ticket MSRC7900.

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

References:

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/497827/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/497825/100/0/threaded>

CVE Reference: [CVE-2008-4788](#)

• CVE-2008-4747 Sun CVSS 2.0 Score = 2.1

Unspecified vulnerability in the search feature in Sun Java System LDAP JDK before 4.20 allows context-dependent attackers to obtain sensitive information via unknown attack vectors related to the LDAP JDK library.

Test Case Impact: Vulnerability Impact: Risk: **Low**

References:

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-26-242246-1>

XF: <http://xforce.iss.net/xforce/xfdb/46074>

SECTRAK: <http://www.securitytracker.com/id?1021103>

BID: <http://www.securityfocus.com/bid/31905>

SECUNIA: <http://secunia.com/advisories/32327>

CVE Reference: [CVE-2008-4747](#)

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