ScoutNews
The weekly Security update from the makers of SecureScout
November 28, 2008

2008 Issue #48

Table of Contents

Product Focus

RPC DCOM Vulnerabilities Scanner - The S4 RPC DCOM Vulnerabilities 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 RPC DCOM flaws (MS03-026 and MS03-039).

Download Here:
http://www.netvigilance.com/productdownloads?productname=rpcdcomvulnerabilitiesscanner

This Week in Review

Increased international coordination expected. Another botnet cut off by ISP.Cybercrime's answer to Friday the 13th. ICANN transfers domains from fraudulent ISP.

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

- **International cooperation focus of SC World Congress panel**

There is some reason for optimism in 2009, especially on the international front, several experts who will be speaking at the SC World Congress say.

Jody Westby (right), CEO of Global Cyber Risk, a Washington, D.C.-based advisory firm, says she expects increased global coordination to deter problems, such as cross-border cyberattacks - similar to what occurred in Estonia after the government there removed a Russian World War II monument.

Information-sharing and resolving jurisdictional and extradition issues are keys to stopping cybercrime. "When you have countries that don't cooperate, the trail goes cold," she says.

SC Magazine

Full Story :
http://www.scmagazineus.com/International-cooperation-focus-of-SC-World-Congress-panel/article/121457/

- **Estonian ISP cuts off control servers for Srizbi botnet**

November 27, 2008 (IDG News Service) An Estonian ISP that temporarily hosted the command-and-control servers for the Srizbi botnet, responsible for a large portion of the world's spam, has cut off those servers, according to computer security analysts.

Hundreds of thousands of PCs around the world infected with Srizbi, a difficult-to-remove rootkit that is used for sending spam, were programmed to seek new instructions from servers in those domains.

But spammers lost control of Srizbi when the ISP that previously hosted its command-and-control servers was cut off from the Internet. McColo, whose servers are based in San Jose, California, was cut off by its upstream providers earlier this month after being exposed by computer security experts and the Washington Post.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9121758&source=rss_topic1

- **Cybercriminals gearing up for Cyber Monday**

Cyber Monday is just days away and cybercriminals are preparing for it like an athlete would for Super Bowl Sunday, one security professional said.

"Cyber Monday" is the cyber-equivalent of "Black Friday" in the brick-and-mortar world. It occurs Dec. 1, the Monday after Thanksgiving -- one of the biggest online shopping days of the year.

Attackers will be creating fake e-commerce sites hoping users will voluntarily hand over their information, a socially engineered cyberattack, as opposed to more elaborate, technical methods in a cybercriminal's arsenal.

SC Magazine

Full Story :
http://www.scmagazineus.com/Cybercriminals-gearing-up-for-Cyber-Monday/article/121597/

- **ICANN to transfer 281,000 domains to new registrar**

The Internet Corp. for Assigned Names and Numbers (ICANN) said Tuesday it will transfer about 281,000 domains that formerly were managed by a registrar whose right to issue new addresses was revoked last month.

Estonia-based EstDomains was de-accredited Oct. 28 after it emerged that its president had been convicted of credit card fraud, money laundering and document forgery. ICANN rules allow it to end accreditation agreements with any registrar whose director is convicted of financial crimes.

ICANN said in a statement that it will transfer the domains to an accredited registrar, India-based Directi Internet Solutions, which will notify customers and provide transfer instructions. Registrants will not be charged for the transfer, expected to be complete by Dec. 1.

SC Magazine

Full Story :
http://www.scmagazineus.com/ICANN-to-transfer-281000-domains-to-new-registrar/article/121534/

New Vulnerabilities Tested in SecureScout

- **18173 Apache mod_imagemap and mod_imap Cross-Site Scripting Vulnerability**

Apache is prone to a cross-site scripting vulnerability because the application fails to properly sanitize user-supplied input.

An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may help the attacker steal cookie-based authentication credentials and launch other attacks.

This issue is fixed in versions 1.3.41, 2.0.63, and 2.2.8.

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

References:

* BUGTRAQ: 20080716 rPSA-2008-0035-1 httpd mod_ssl
http://www.securityfocus.com/archive/1/archive/1/494428/100/0/threaded
* 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://www.fujitsu.com/global/support/software/security/products-f/interstage-200801e.html
* CONFIRM:
http://support.avaya.com/elmodocs2/security/ASA-2008-032.htm
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=307562
* AIXAPAR: PK58024
http://www-1.ibm.com/support/docview.wss?uid=swg1PK58024
* AIXAPAR: PK58074
http://www-1.ibm.com/support/docview.wss?uid=swg1PK58074
* AIXAPAR: PK63273
http://www-1.ibm.com/support/docview.wss?uid=swg1PK63273
* AIXAPAR: PK65782
http://www-1.ibm.com/support/docview.wss?uid=swg24019245
* APPLE: APPLE-SA-2008-03-18
http://lists.apple.com/archives/security-announce/2008/Mar/msg00001.html
* APPLE: APPLE-SA-2008-05-28
http://lists.apple.com/archives/security-announce/2008//May/msg00001.html
* FEDORA: FEDORA-2008-1695
https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00562.html
* FEDORA: FEDORA-2008-1711
https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00541.html
* HP: HPSBUX02308
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01345501
* MANDRIVA: MDVSA-2008:014
http://www.mandriva.com/security/advisories?name=MDVSA-2008:014
* MANDRIVA: MDVSA-2008:015
http://www.mandriva.com/security/advisories?name=MDVSA-2008:015
* MANDRIVA: MDVSA-2008:016
http://www.mandriva.com/security/advisories?name=MDVSA-2008:016
* REDHAT: RHSA-2008:0004
http://www.redhat.com/support/errata/RHSA-2008-0004.html
* REDHAT: RHSA-2008:0005
http://www.redhat.com/support/errata/RHSA-2008-0005.html
* REDHAT: RHSA-2008:0006
http://www.redhat.com/support/errata/RHSA-2008-0006.html
* REDHAT: RHSA-2008:0007
http://www.redhat.com/support/errata/RHSA-2008-0007.html
* REDHAT: RHSA-2008:0008
http://www.redhat.com/support/errata/RHSA-2008-0008.html
* REDHAT: RHSA-2008:0009
http://www.redhat.com/support/errata/RHSA-2008-0009.html
* REDHAT: RHSA-2008:0261
http://www.redhat.com/support/errata/RHSA-2008-0261.html
* SLACKWARE: SSA:2008-045-02
http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.595748
* SUNALERT: 233623
http://sunsolve.sun.com/search/document.do?assetkey=1-26-233623-1
* SUSE: SUSE-SA:2008:021
http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00004.html
* UBUNTU: USN-575-1
http://www.ubuntu.com/usn/usn-575-1
* CERT: TA08-150A
http://www.us-cert.gov/cas/techalerts/TA08-150A.html
* BID: 26838
http://www.securityfocus.com/bid/26838
* FRSIRT: ADV-2007-4201
http://www.frsirt.com/english/advisories/2007/4201
* FRSIRT: ADV-2007-4202
http://www.frsirt.com/english/advisories/2007/4202
* FRSIRT: ADV-2007-4301

http://www.frsirt.com/english/advisories/2007/4301
* FRSIRT: ADV-2008-0084
http://www.frsirt.com/english/advisories/2008/0084
* FRSIRT: ADV-2008-0178
http://www.frsirt.com/english/advisories/2008/0178
* FRSIRT: ADV-2008-0398
http://www.frsirt.com/english/advisories/2008/0398
* FRSIRT: ADV-2008-0809
http://www.frsirt.com/english/advisories/2008/0809/references
* FRSIRT: ADV-2008-0924
http://www.frsirt.com/english/advisories/2008/0924/references
* FRSIRT: ADV-2008-1224
http://www.frsirt.com/english/advisories/2008/1224/references
* FRSIRT: ADV-2008-1623
http://www.frsirt.com/english/advisories/2008/1623/references
* FRSIRT: ADV-2008-1697
http://www.frsirt.com/english/advisories/2008/1697
* FRSIRT: ADV-2008-1875
http://www.frsirt.com/english/advisories/2008/1875/references
* OSVDB: 39134
http://www.osvdb.org/39134
* SECTRACK: 1019093
http://securitytracker.com/id?1019093
* SECUNIA: 28046
http://secunia.com/advisories/28046
* SECUNIA: 28073
http://secunia.com/advisories/28073
* SECUNIA: 28081
http://secunia.com/advisories/28081
* SECUNIA: 28196
http://secunia.com/advisories/28196
* SECUNIA: 28375
http://secunia.com/advisories/28375
* SECUNIA: 28467
http://secunia.com/advisories/28467
* SECUNIA: 28471
http://secunia.com/advisories/28471
* SECUNIA: 28525
http://secunia.com/advisories/28525
* SECUNIA: 28526
http://secunia.com/advisories/28526
* SECUNIA: 28607
http://secunia.com/advisories/28607
* SECUNIA: 28749
http://secunia.com/advisories/28749
* SECUNIA: 28750
http://secunia.com/advisories/28750
* SECUNIA: 28977
http://secunia.com/advisories/28977
* SECUNIA: 28922
http://secunia.com/advisories/28922
* SECUNIA: 29420
http://secunia.com/advisories/29420
* SECUNIA: 29640
http://secunia.com/advisories/29640
* SECUNIA: 29806
http://secunia.com/advisories/29806
* SECUNIA: 29988
http://secunia.com/advisories/29988
* SECUNIA: 30356
http://secunia.com/advisories/30356
* SECUNIA: 30430
http://secunia.com/advisories/30430
* SECUNIA: 31142
http://secunia.com/advisories/31142
* XF: apache-modimagemap-xss(39002)
http://xforce.iss.net/xforce/xfdb/39002
* XF: apache-modimap-xss(39001)
http://xforce.iss.net/xforce/xfdb/39001

CVE Reference:

CVE-2007-5000 (cve.mitre.org, nvd.nist.gov)

- **18175 Apache HTTP Server 413 error page cross-site scripting**

Apache HTTP Server does not sanitize the HTTP Method specifier header from an HTTP request when it is reflected back in a "413 Request Entity Too Large" error message, which might allow cross-site scripting (XSS) style attacks using web client components that can send arbitrary headers in requests, as demonstrated via an HTTP request containing an invalid Content-length value.
An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

The issue has been fixed in version 2.2.5 and 2.0.60.

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

References:

* MISC: The Apache HTTP Server Project
http://httpd.apache.org/
* BUGTRAQ: 20071130 PR07-37: XSS on Apache HTTP Server 413 error pages via malformed HTTP method
http://www.securityfocus.com/archive/1/archive/1/484410/100/0/threaded
* MISC:
http://procheckup.com/Vulnerability_PR07-37.php
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=307562
* AIXAPAR: PK57952
http://www-1.ibm.com/support/docview.wss?uid=swg1PK57952
* AIXAPAR: PK65782
http://www-1.ibm.com/support/docview.wss?uid=swg24019245
* APPLE: APPLE-SA-2008-03-18
http://lists.apple.com/archives/security-announce/2008/Mar/msg00001.html
* GENTOO: GLSA-200803-19
http://security.gentoo.org/glsa/glsa-200803-19.xml
* SUSE: SUSE-SA:2008:021
http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00004.html
* BID: 26663
http://www.securityfocus.com/bid/26663
* FRSIRT: ADV-2007-4060
http://www.frsirt.com/english/advisories/2007/4060
* FRSIRT: ADV-2007-4301
http://www.frsirt.com/english/advisories/2007/4301
* FRSIRT: ADV-2008-0924
http://www.frsirt.com/english/advisories/2008/0924/references
* FRSIRT: ADV-2008-1623
http://www.frsirt.com/english/advisories/2008/1623/references
* FRSIRT: ADV-2008-1875
http://www.frsirt.com/english/advisories/2008/1875/references
* SECTRACK: 1019030
http://www.securitytracker.com/id?1019030
* SECUNIA: 27906
http://secunia.com/advisories/27906
* SECUNIA: 28196
http://secunia.com/advisories/28196
* SECUNIA: 29348
http://secunia.com/advisories/29348
* SECUNIA: 29420
http://secunia.com/advisories/29420
* SECUNIA: 29640
http://secunia.com/advisories/29640
* SECUNIA: 30356
http://secunia.com/advisories/30356
* SREASON: 3411
http://securityreason.com/securityalert/3411
* XF: apache-413error-xss(38800)
http://xforce.iss.net/xforce/xfdb/38800

CVE Reference:

CVE-2007-6203 (cve.mitre.org, nvd.nist.gov)

- **18176 Apache HTTP Server 'mod_status' Cross-Site Scripting Vulnerability**

The Apache HTTP Server 'mod_status' module is prone to a cross-site scripting vulnerability because the application fails to properly sanitize user-supplied input.

An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks. Reportedly, attackers can also use this issue to redirect users' browsers to arbitrary locations, which may aid in phishing attacks.

The issue has been fixed in versions 1.3.41, 2.0.63, and 2.2.8.

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

References:

* MISC: The Apache HTTP Server Project
http://httpd.apache.org/
* BUGTRAQ: 20080716 rPSA-2008-0035-1 httpd mod_ssl
http://www.securityfocus.com/archive/1/archive/1/494428/100/0/threaded
* 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-2008-032.htm
* CONFIRM:
http://support.nortel.com/go/main.jsp?cscat=BLTNDETAIL&id=689039
* CONFIRM:
http://www116.nortel.com/pub/repository/CLARIFY/DOCUMENT/2008/05/023342-01.pdf
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=307562
* AIXAPAR: PK59667
http://www-1.ibm.com/support/search.wss?rs=0&q=PK59667&apar=only
* AIXAPAR: PK62966
http://www-1.ibm.com/support/docview.wss?uid=swg1PK62966
* AIXAPAR: PK63273
http://www-1.ibm.com/support/docview.wss?uid=swg1PK63273
* AIXAPAR: PK65782
http://www-1.ibm.com/support/docview.wss?uid=swg24019245
* APPLE: APPLE-SA-2008-03-18
http://lists.apple.com/archives/security-announce/2008/Mar/msg00001.html
* APPLE: APPLE-SA-2008-05-28
http://lists.apple.com/archives/security-announce/2008//May/msg00001.html
* FEDORA: FEDORA-2008-1695
https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00562.html
* FEDORA: FEDORA-2008-1711
https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00541.html
* HP: HPSBUX02313
http://www.securityfocus.com/archive/1/archive/1/488082/100/0/threaded
* MANDRIVA: MDVSA-2008:014
http://www.mandriva.com/security/advisories?name=MDVSA-2008:014
* MANDRIVA: MDVSA-2008:015
http://www.mandriva.com/security/advisories?name=MDVSA-2008:015
* MANDRIVA: MDVSA-2008:016
http://www.mandriva.com/security/advisories?name=MDVSA-2008:016
* REDHAT: RHSA-2008:0004
http://www.redhat.com/support/errata/RHSA-2008-0004.html
* REDHAT: RHSA-2008:0005
http://www.redhat.com/support/errata/RHSA-2008-0005.html
* REDHAT: RHSA-2008:0006
http://www.redhat.com/support/errata/RHSA-2008-0006.html
* REDHAT: RHSA-2008:0007
http://www.redhat.com/support/errata/RHSA-2008-0007.html
* REDHAT: RHSA-2008:0008
http://www.redhat.com/support/errata/RHSA-2008-0008.html
* REDHAT: RHSA-2008:0009
http://www.redhat.com/support/errata/RHSA-2008-0009.html
* REDHAT: RHSA-2008:0261
http://www.redhat.com/support/errata/RHSA-2008-0261.html

* SLACKWARE: SSA:2008-045-02
http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.595748
* SUNALERT: 233623
http://sunsolve.sun.com/search/document.do?assetkey=1-26-233623-1
* SUSE: SUSE-SA:2008:021
http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00004.html
* UBUNTU: USN-575-1
http://www.ubuntu.com/usn/usn-575-1
* CERT: TA08-150A
http://www.us-cert.gov/cas/techalerts/TA08-150A.html
* BID: 27237
http://www.securityfocus.com/bid/27237
* FRSIRT: ADV-2008-0047
http://www.frsirt.com/english/advisories/2008/0047
* FRSIRT: ADV-2008-0447
http://www.frsirt.com/english/advisories/2008/0447/references
* FRSIRT: ADV-2008-0554
http://www.frsirt.com/english/advisories/2008/0554
* FRSIRT: ADV-2008-0809
http://www.frsirt.com/english/advisories/2008/0809/references
* FRSIRT: ADV-2008-0924
http://www.frsirt.com/english/advisories/2008/0924/references
* FRSIRT: ADV-2008-0986
http://www.frsirt.com/english/advisories/2008/0986/references
* FRSIRT: ADV-2008-1224
http://www.frsirt.com/english/advisories/2008/1224/references
* FRSIRT: ADV-2008-1623
http://www.frsirt.com/english/advisories/2008/1623/references
* FRSIRT: ADV-2008-1697
http://www.frsirt.com/english/advisories/2008/1697
* SECTRACK: 1019154
http://securitytracker.com/id?1019154
* SECUNIA: 28467
http://secunia.com/advisories/28467
* SECUNIA: 28471
http://secunia.com/advisories/28471
* SECUNIA: 28526
http://secunia.com/advisories/28526
* SECUNIA: 28607
http://secunia.com/advisories/28607
* SECUNIA: 28749
http://secunia.com/advisories/28749
* SECUNIA: 28965
http://secunia.com/advisories/28965
* SECUNIA: 28977
http://secunia.com/advisories/28977
* SECUNIA: 28922
http://secunia.com/advisories/28922
* SECUNIA: 29420
http://secunia.com/advisories/29420
* SECUNIA: 29504
http://secunia.com/advisories/29504
* SECUNIA: 29640
http://secunia.com/advisories/29640
* SECUNIA: 29806
http://secunia.com/advisories/29806
* SECUNIA: 29988
http://secunia.com/advisories/29988
* SECUNIA: 30356
http://secunia.com/advisories/30356
* SECUNIA: 30430
http://secunia.com/advisories/30430
* SECUNIA: 31142
http://secunia.com/advisories/31142
* SREASON: 3541
http://securityreason.com/securityalert/3541
* XF: apache-status-page-xss(39472)
http://xforce.iss.net/xforce/xfdb/39472

CVE Reference:

CVE-2007-6388 (cve.mitre.org, nvd.nist.gov)

- **18177 Apache HTTP Server mod_proxy_balancer cross-site scripting**

Apache HTTP Server is vulnerable to a Cross-site scripting (XSS) vulnerability in balancer-manager, caused by improper validation of user-supplied input by the mod_proxy_balancer module. A remote attacker could exploit this vulnerability using the (1) ss, (2) wr, or (3) rr parameters, or (4) the URL in a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

The issue has been fixed in version 2.2.8.

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

References:

* MISC: The Apache HTTP Server Project
http://httpd.apache.org/
* BUGTRAQ: 20080716 rPSA-2008-0035-1 httpd mod_ssl
http://www.securityfocus.com/archive/1/archive/1/494428/100/0/threaded
* 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-2008-032.htm
* CONFIRM:
http://support.nortel.com/go/main.jsp?cscat=BLTNDETAIL&id=689039
* CONFIRM:
http://www116.nortel.com/pub/repository/CLARIFY/DOCUMENT/2008/05/023342-01.pdf
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=307562
* AIXAPAR: PK59667
http://www-1.ibm.com/support/search.wss?rs=0&q=PK59667&apar=only
* AIXAPAR: PK62966
http://www-1.ibm.com/support/docview.wss?uid=swg1PK62966
* AIXAPAR: PK63273
http://www-1.ibm.com/support/docview.wss?uid=swg1PK63273
* AIXAPAR: PK65782
http://www-1.ibm.com/support/docview.wss?uid=swg24019245
* APPLE: APPLE-SA-2008-03-18
http://lists.apple.com/archives/security-announce/2008/Mar/msg00001.html
* APPLE: APPLE-SA-2008-05-28
http://lists.apple.com/archives/security-announce/2008//May/msg00001.html
* FEDORA: FEDORA-2008-1695
https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00562.html
* FEDORA: FEDORA-2008-1711
https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00541.html
* HP: HPSBUX02313
http://www.securityfocus.com/archive/1/archive/1/488082/100/0/threaded
* MANDRIVA: MDVSA-2008:014
http://www.mandriva.com/security/advisories?name=MDVSA-2008:014
* MANDRIVA: MDVSA-2008:015
http://www.mandriva.com/security/advisories?name=MDVSA-2008:015
* MANDRIVA: MDVSA-2008:016
http://www.mandriva.com/security/advisories?name=MDVSA-2008:016
* REDHAT: RHSA-2008:0004
http://www.redhat.com/support/errata/RHSA-2008-0004.html
* REDHAT: RHSA-2008:0005
http://www.redhat.com/support/errata/RHSA-2008-0005.html
* REDHAT: RHSA-2008:0006
http://www.redhat.com/support/errata/RHSA-2008-0006.html
* REDHAT: RHSA-2008:0007
http://www.redhat.com/support/errata/RHSA-2008-0007.html
* REDHAT: RHSA-2008:0008
http://www.redhat.com/support/errata/RHSA-2008-0008.html
* REDHAT: RHSA-2008:0009
http://www.redhat.com/support/errata/RHSA-2008-0009.html
* REDHAT: RHSA-2008:0261

http://www.redhat.com/support/errata/RHSA-2008-0261.html
* SLACKWARE: SSA:2008-045-02
http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.595748
* SUNALERT: 233623
http://sunsolve.sun.com/search/document.do?assetkey=1-26-233623-1
* SUSE: SUSE-SA:2008:021
http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00004.html
* UBUNTU: USN-575-1
http://www.ubuntu.com/usn/usn-575-1
* CERT: TA08-150A
http://www.us-cert.gov/cas/techalerts/TA08-150A.html
* BID: 27237
http://www.securityfocus.com/bid/27237
* FRSIRT: ADV-2008-0047
http://www.frsirt.com/english/advisories/2008/0047
* FRSIRT: ADV-2008-0447
http://www.frsirt.com/english/advisories/2008/0447/references
* FRSIRT: ADV-2008-0554
http://www.frsirt.com/english/advisories/2008/0554
* FRSIRT: ADV-2008-0809
http://www.frsirt.com/english/advisories/2008/0809/references
* FRSIRT: ADV-2008-0924
http://www.frsirt.com/english/advisories/2008/0924/references
* FRSIRT: ADV-2008-0986
http://www.frsirt.com/english/advisories/2008/0986/references
* FRSIRT: ADV-2008-1224
http://www.frsirt.com/english/advisories/2008/1224/references
* FRSIRT: ADV-2008-1623
http://www.frsirt.com/english/advisories/2008/1623/references
* FRSIRT: ADV-2008-1697
http://www.frsirt.com/english/advisories/2008/1697
* SECTRACK: 1019154
http://securitytracker.com/id?1019154
* SECUNIA: 28467
http://secunia.com/advisories/28467
* SECUNIA: 28471
http://secunia.com/advisories/28471
* SECUNIA: 28526
http://secunia.com/advisories/28526
* SECUNIA: 28607
http://secunia.com/advisories/28607
* SECUNIA: 28749
http://secunia.com/advisories/28749
* SECUNIA: 28965
http://secunia.com/advisories/28965
* SECUNIA: 28977
http://secunia.com/advisories/28977
* SECUNIA: 28922
http://secunia.com/advisories/28922
* SECUNIA: 29420
http://secunia.com/advisories/29420
* SECUNIA: 29504
http://secunia.com/advisories/29504
* SECUNIA: 29640
http://secunia.com/advisories/29640

CVE Reference:

CVE-2007-6421 (cve.mitre.org, nvd.nist.gov)

• 18195 Cisco IOS NAT Skinny Call Control Protocol Vulnerability (cisco-sa-20080924-sccp)

The Skinny Call Control Protocol (SCCP) enables voice communication between an SCCP client and a Call Manager (CM). Typically, the CM provides service to the SCCP clients on TCP Port 2000 by default. Initially, an SCCP client connects to the CM by establishing a TCP connection; the client will also establish a TCP connection with a secondary CM, if available.

The NAT SCCP Fragmentation Support feature prevents skinny control message exchanges from failing in a TCP segmentation scenario because the NAT Skinny Application Layer Gateway (ALG) is able to reassemble the skinny control messages. A segmented payload that requires an IP or port translation will no longer be dropped. The NAT SCCP Fragmentation Support feature was introduced in Cisco IOS version 12.4(6)T.

A series of fragmented SCCP messages may cause a Cisco IOS router that is running the NAT SCCP Fragmentation Support feature to reload.

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

References:

* CISCO: 20080924 Cisco IOS NAT Skinny Call Control Protocol Vulnerability
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a0148e.shtml

CVE Reference:

CVE-2008-3810 (cve.mitre.org, nvd.nist.gov)
CVE-2008-3811 (cve.mitre.org, nvd.nist.gov)

• 18196 Multiple Cisco IOS Session Initiation Protocol Denial of Service Vulnerabilities (cisco-sa-20080924-sip)

SIP is a popular signaling protocol used to manage voice and video calls across IP networks such as the Internet. SIP is responsible for handling all aspects of call setup and termination. Voice and video are the most popular types of sessions that SIP handles, but the protocol is flexible to accommodate for other applications that require call setup and termination. SIP call signaling can use UDP (port 5060), TCP (port 5060), or TLS (TCP port 5061) as the underlying transport protocol.

Multiple denial of service vulnerabilities exist in the SIP implementation in Cisco IOS. In all cases vulnerabilities can be triggered by processing valid SIP messages.

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

References:

* CISCO: 20080924 Multiple Cisco IOS Session Initiation Protocol Denial of Service Vulnerabilities
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a01562.shtml
* CISCO: 20080924 Cisco Unified Communications Manager Session Initiation Protocol Denial of Service Vulnerabilities
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a0156a.shtml

CVE Reference:

CVE-2008-3799 (cve.mitre.org, nvd.nist.gov)
CVE-2008-3800 (cve.mitre.org, nvd.nist.gov)
CVE-2008-3801 (cve.mitre.org, nvd.nist.gov)
CVE-2008-3802 (cve.mitre.org, nvd.nist.gov)

• 18197 Cisco IOS IPS Denial of Service Vulnerability (cisco-sa-20080924-iosips)

Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection feature that effectively mitigates a wide range of network attacks. A component of the Cisco IOS Integrated Threat Control framework and complemented by Cisco IOS Flexible Packet Matching feature, Cisco IOS IPS provides your network with the intelligence to accurately identify, classify, and stop or block malicious traffic in real time. Additional information on the Cisco IOS IPS feature can be found at http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_fwids.html.

Previous to the introduction of the Cisco IOS IPS feature, Cisco IOS provided a similar feature, the Cisco IOS Intrusion Detection System (IDS). The Cisco IOS IDS feature is not affected by this vulnerability. Additional information on the Cisco IOS IDS feature can be found at http://www.cisco.com/en/US/docs/ios/12_0t/12_0t5/feature/guide/ios_ids.html.

Certain network traffic can trigger IPS signatures on the SERVICE.DNS signature engine which may cause the Cisco IOS device to crash or hang. This may cause a denial of service that results in disruption of network traffic. This vulnerability is documented in Cisco Bug ID CSCsq13348 (registered customers only) .

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

References:

* CISCO: 20080924 Cisco IOS IPS Denial of Service Vulnerability
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a01556.shtml

CVE Reference:

CVE-2008-2739 (cve.mitre.org, nvd.nist.gov)

• 18198 Cisco IOS MPLS VPN May Leak Information (cisco-sa-20080924-vpn)

MPLS VPNs allow for the creation of 'virtual networks' that customers can use to segregate traffic into multiple, isolated VPNs. Traffic within each MPLS VPN is kept separate from the others, thereby maintaining a virtual private network.

More information on MPLS and MPLS VPNs is available at the following link:

http://www.cisco.com/en/US/products/ps6557/products_ios_technology_home.html

A bug exists when processing extended communities with MPLS VPNs. If extended communities are used, MPLS VPN may incorrectly use a corrupted route target (RT) to forward traffic. If this occurs, traffic can leak from one MPLS VPN to another.

This vulnerability exists whenever an affected PE device has a BGP session running in the MPLS VPN Virtual Routing and Forwarding (VRF). The following two examples of this scenario are the most common:

1) MPLS VPN configuration with BGP running inside the VRF between the PE and CE devices.

2) MPLS Inter-AS option A with BGP running between the Autonomous System Border Routers (ASBR).

The mitigation in the Workarounds section filters extended communities on a PE device, preventing them from being received by devices configured for MPLS VPN.

This vulnerability was introduced with Cisco bug ID CSCee83237. Cisco IOS images that do not include CSCee83237 are not vulnerable to this issue.

It is important to note that this condition cannot be triggered by an attacker and that the condition does not provide ways to determine the flow of traffic between VPNs.

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

References:

* CISCO: 20080924 Cisco IOS MPLS VPN May Leak Information
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a014a9.shtml

CVE Reference:

CVE-2008-3803 (cve.mitre.org, nvd.nist.gov)

• 18199 Cisco IOS MPLS Forwarding Infrastructure Denial of Service Vulnerability (cisco-sa-20080924-mfi)

In newer versions of Cisco IOS software, a new packet forwarding infrastructure was introduced to improve scalability and performance. This forwarding infrastructure, called MFI, is transparent to the user. MFI manages MPLS data structures used for forwarding and replaces the older implementation, Label Forwarding Information Base (LFIB). Cisco IOS MFI implementation is vulnerable to a DoS attack from specially crafted packets that are handled in the software path, including transit packets that are handled in the software path. Such packets can be sent from the local segment to the interfaces that are configured for MPLS or via tunnel interfaces that are configured for MPLS. To target a remote system in an MPLS network, an attacker needs to have access to the MPLS network through an MPLS-enabled interface. MPLS packets are dropped on interfaces that are not configured for MPLS.

Devices that support MFI will have mfi_ios in the output of the show subsys command. Interfaces that are enabled for MPLS can be seen by the show mpls interface command.

More information on MFI can be found at the following link:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_lsc_removed.html

This vulnerability is documented in the Cisco Bug ID CSCsk93241.

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

References:

* CISCO: 20080924 Cisco IOS MPLS Forwarding Infrastructure Denial of Service Vulnerability
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a014ac.shtml

CVE Reference:

CVE-2008-3804 (cve.mitre.org, nvd.nist.gov)

• 18200 Cisco 10000, uBR10012, uBR7200 Series Devices IPC Vulnerability (cisco-sa-20080924-ipc)

Cisco 10000, uBR10012 and uBR7200 series devices use a UDP-based IPC channel. This channel uses addresses from the 127.0.0.0/8 range and UDP port 1975. Cisco 10000, uBR10012 and uBR7200 series devices that are running an affected version of Cisco IOS will process IPC messages that are sent to UDP port 1975 from outside of the device. This behavior may be exploited by an attacker to cause a reload of the device, linecards, or both, resulting in a DoS condition.

Filtering unauthorized traffic destined to 127.0.0.0/8 or UDP port 1975 will mitigate this vulnerability.

This vulnerability is documented in the Cisco Bug IDs CSCsg15342 and CSCsh29217.

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

References:

* CONFIRM:
http://tools.cisco.com/security/center/viewAlert.x?alertId=16646
* CISCO: 20080924 Cisco 10000, uBR10012, uBR7200 Series Devices IPC Vulnerability
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a014ae.shtml
* XF: ios-udp-ipc-dos-variant2(45592)
http://xforce.iss.net/xforce/xfdb/45592

CVE Reference:

CVE-2008-3805 (cve.mitre.org, nvd.nist.gov)
CVE-2008-3806 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2008-5232 Microsoft CVSS 2.0 Score = 9.3

Buffer overflow in the CallHTMLHelp method in the Microsoft Windows Media Services ActiveX control in nskey.dll 4.1.00.3917 in Windows Media Services on Microsoft Windows NT and 2000, and Avaya Media and Message Application servers, allows remote attackers to execute arbitrary code via a long argument. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.

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

References:

MISC: http://www.securityfocus.com/data/vulnerabilities/exploits/30814.html.txt

BID: http://www.securityfocus.com/bid/30814

CVE Reference: CVE-2008-5232

• CVE-2008-5229 Microsoft CVSS 2.0 Score = 6.9

Stack-based buffer overflow in Microsoft Device IO Control in iphlpapi.dll in Microsoft Windows Vista Gold and SP1 allows local users in the Network Configuration Operator group to gain privileges or cause a denial of service (system crash) via a large invalid PrefixLength to the CreateIpForwardEntry2 method, as demonstrated by a "route add" command.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/46742

BID: http://www.securityfocus.com/bid/32357

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/498471/100/0/threaded

SECTRACK: http://securitytracker.com/id?1021245

CVE Reference: CVE-2008-5229

• CVE-2008-5230 Cisco CVSS 2.0 Score = 6.8

The Temporal Key Integrity Protocol (TKIP) implementation in unspecified Cisco products and other vendors' products, as used in WPA and WPA2 on Wi-Fi networks, has insufficient countermeasures against certain crafted and replayed packets, which makes it easier for remote attackers to decrypt packets from an access point (AP) to a client and spoof packets from an AP to a client, and conduct ARP poisoning attacks or other attacks, as demonstrated by

tkiptun-ng.

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

References:

BID: http://www.securityfocus.com/bid/32164

CISCO: http://www.cisco.com/en/US/products/products_security_response09186a0080a30036.html

MISC: http://www.aircrack-ng.org/doku.php?id=tkiptun-ng

MISC: http://trac.aircrack-ng.org/svn/trunk/src/tkiptun-ng.c

MISC: http://radajo.blogspot.com/2008/11/wpatkip-chopchop-attack.html

MLIST: http://lists.immunitysec.com/pipermail/dailydave/2008-November/005413.html

MISC: http://dl.aircrack-ng.org/breakingwepandwpa.pdf

MISC: http://arstechnica.com/articles/paedia/wpa-cracked.ars

CVE Reference: CVE-2008-5230

- **CVE-2008-4231 Apple CVSS 2.0 Score = 9.3**

Safari in Apple iPhone OS 1.0 through 2.1 and iPhone OS for iPod touch 1.1 through 2.1 does not properly handle HTML TABLE elements, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted HTML document.

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

References:

BID: http://www.securityfocus.com/bid/32394

CONFIRM: http://support.apple.com/kb/HT3318

APPLE: http://lists.apple.com/archives/security-announce/2008/Nov/msg00002.html

CVE Reference: CVE-2008-4231

- **CVE-2008-2431 Novell CVSS 2.0 Score = 9.3**

Multiple buffer overflows in Novell iPrint Client before 5.06 allow remote attackers to execute arbitrary code by calling the Novell iPrint ActiveX control (aka ienipp.ocx) with (1) a long third argument to the GetDriverFile method; a long first argument to the (2) GetPrinterURLList or (3) GetPrinterURLList2 method; (4) a long argument to the GetFileList method; a long argument to the (5) GetServerVersion, (6) GetResourceList, or (7) DeleteResource method, related to nipplib.dll; a long uploadPath argument to the (8) UploadPrinterDriver or (9) UploadResource method, related to URIs; (10) a long seventh argument to the UploadResource method; a long string in the (11) second, (12) third, or (13) fourth argument to the GetDriverSettings method, related to the IppGetDriverSettings function in nipplib.dll; or (14) a long eighth argument to the UploadResourceToRMS method.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/44616

BID: http://www.securityfocus.com/bid/30813

MISC: http://secunia.com/secunia_research/2008-27/advisory/

SECUNIA: http://secunia.com/advisories/30667

CVE Reference: CVE-2008-2431

- **CVE-2008-5231 Novell CVSS 2.0 Score = 9.3**

Stack-based buffer overflow in the ExecuteRequest method in the Novell iPrint ActiveX control in ienipp.ocx in Novell iPrint Client 5.06 and earlier allows remote attackers to execute arbitrary code via a long target-frame option value, a different vulnerability than CVE-2008-2431.

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

References:

BID: http://www.securityfocus.com/bid/30813

MISC: http://secunia.com/secunia_research/2008-27/advisory/

SECUNIA: http://secunia.com/advisories/30667

CVE Reference: CVE-2008-5231

- **CVE-2008-4227 Apple CVSS 2.0 Score = 7.5**

Apple iPhone OS 1.0 through 2.1 and iPhone OS for iPod touch 1.1 through 2.1 changes the encryption level of PPTP VPN connections to a lower level that was previously used, which makes it easier for remote attackers to obtain sensitive information or hijack a connection by decrypting network traffic.

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

References:

BID: http://www.securityfocus.com/bid/32394

CONFIRM: http://support.apple.com/kb/HT3318

APPLE: http://lists.apple.com/archives/security-announce/2008/Nov/msg00002.html

CVE Reference: CVE-2008-4227

- **CVE-2008-4636 Novell CVSS 2.0 Score = 7.2**

yast2-backup 2.14.2 through 2.16.6 on SUSE Linux and Novell Linux allows local users to gain privileges via shell metacharacters in filenames used by the backup process.

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

References:

BID: http://www.securityfocus.com/bid/32464

SUSE: http://lists.opensuse.org/opensuse-security-announce/2008-11/msg00003.html

SECUNIA: http://secunia.com/advisories/32832

CVE Reference: CVE-2008-4636

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