

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

[WinArpd v1.0b8](#) - Download WinArpd executable by filling our download form. Size: 55KB

Download Here:

<http://www.netvigilance.com/productdownloads?productname=winarpd.exe.zip>

This Week in Review

Review of US federal cybersecurity policies. Survey shows IT pros cheat on audits. US military goes cyber. Spam=90% of mails in May.

Note from the techies:

SecureScout NX has been improved and is now less resource intensive when loading.

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

• Setting cybersecurity as a national priority is just the beginning

A review of federal cybersecurity policies, scheduled for release Friday, will serve as a call to action for the public and private sectors, said Dale Meyerrose, vice president and general manager of cyber and information assurance at Harris Corp., a communications and information technology company.

Meyerrose spoke Tuesday night at a gathering at the New York Press Club in Manhattan on the topic of "The State of Cyberspace in America."

SC Magazine

Full Story :

<http://www.scmagazineus.com/Setting-cybersecurity-as-a-national-priority-is-just-the-beginning/article/137528/>

• Study finds IT security pros cheat on audits

IT security professionals might think of auditing as a pain, but some are actually cheating to get audits passed, according to a study released Wednesday by security vendor Tufin Technologies.

According to the survey of 150 IT security managers and technical staff from enterprises and government departments, 20 percent admitted to cheating on security audits or knowing of a colleague that did. The survey was conducted from April 28 to 30 during InfoSecurity Europe in London.

Ruvi Kitov, CEO of Tufin Technologies, told SCMagazineUS.com Wednesday that with self-audits, security practitioners have to run through a set of checks and fill out a form verifying they accomplished certain tasks. Some, though, erroneously fill out the forms to cut corners, Kitov said. In other cases, IT security professionals might lie to an external auditor, who does not follow up to ensure the answers are valid.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Study-finds-IT-security-pros-cheat-on-audits/article/137546/>

• **New cyberattack technologies developed for U.S. military**

The U.S. military is developing and testing several new offensive and defense cyberdevices, including a system that would enable non-expert military personnel to launch a cyberattack, a defense and aerospace industry publication reported last week.

One of the devices would be able to tap into wireless networks, including satellite communications, voice over IP and SCADA (Supervisory Control and Data Acquisition) networks to test for vulnerabilities to penetration, Aviation Week reported.

Because few people currently understand how to launch or respond to a cyberattack, some of the technologies are being tailored for a non-expert use, according to the story. The devices are being built in a "U.S. cyberwarfare attack laboratory."

SC Magazine

Full Story :

<http://www.scmagazineus.com/New-cyberattack-technologies-developed-for-US-military/article/137451/>

• **Spam accounted for 90 percent of all email in May**

Spam is back on the rise, according to Symantec's MessageLabs monthly report.

The report concluded that in May, the percentage of junk mail jumped 5.1 percent to 90.4 percent. Most of the messages contain nothing more than a subject line and a hyperlink. In many of the cases, the links led to social-networking site profiles, which the spammers likely created en masse by using automated CAPTCHA-breaking tools. The pages typically hawked weight-loss medication.

What makes this spamming technique successful is that the emails are sent from valid accounts hosted by the social-networking provider, according to the report.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Spam-accounted-for-90-percent-of-all-email-in-May/article/137486/>

New Vulnerabilities Tested in SecureScout

• **14504 Adobe Acrobat / Reader getAnnots Doc method in the JavaScript API code execution Vulnerability (Remote File Checking)**

The getAnnots Doc method in the JavaScript API in Adobe Reader and Acrobat 9.1, 8.1.4, 7.1.1, and earlier allows remote attackers to cause a denial of service (memory corruption) or execute arbitrary code via a PDF file that contains an annotation, and has an OpenAction entry with JavaScript code that calls this method with crafted integer arguments.

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

References:

* MILWORM: 8569

<http://www.milw0rm.com/exploits/8569>

* MISC:

http://blogs.adobe.com/psirt/2009/04/potential_adobe_reader_issue.html

* MISC:

<http://packetstorm.linuxsecurity.com/0904-exploits/getannots.txt>

* CONFIRM:

http://blogs.adobe.com/psirt/2009/04/update_on_adobe_reader_issue.html

* CONFIRM:

http://blogs.adobe.com/psirt/2009/05/adobe_reader_issue_update.html

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb09-06.html>

* REDHAT: RHSA-2009:0478

<http://www.redhat.com/support/errata/RHSA-2009-0478.html>

* SUNALERT: 259028

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-259028-1>

* SUSE: SUSE-SA:2009:027

<http://lists.opensuse.org/opensuse-security-announce/2009-05/msg00001.html>

* CERT: TA09-133B

<http://www.us-cert.gov/cas/techalerts/TA09-133B.html>

* CERT-VN: VU#970180

<http://www.kb.cert.org/vuls/id/970180>

* BID: 34736

<http://www.securityfocus.com/bid/34736>

* OSVDB: 54130

<http://osvdb.org/54130>

* SECTRAK: 1022139

<http://www.securitytracker.com/id?1022139>

* SECUNIA: 34924

<http://secunia.com/advisories/34924>

* SECUNIA: 35096

<http://secunia.com/advisories/35096>

* SECUNIA: 35055

<http://secunia.com/advisories/35055>

* SECUNIA: 35152

<http://secunia.com/advisories/35152>

* VUPEN: ADV-2009-1189

<http://www.vupen.com/english/advisories/2009/1189>

* VUPEN: ADV-2009-1317

<http://www.vupen.com/english/advisories/2009/1317>

* XF: reader-getannots-code-execution(50145)

<http://xforce.iss.net/xforce/xfdb/50145>

CVE Reference:

CVE-2009-1492 (cve.mitre.org, nvd.nist.gov)

• 14506 Adobe Acrobat / Reader embedded JBIG2 image stream code execution Vulnerability (Remote File Checking)

Buffer overflow in Adobe Reader 9.0 and earlier, and Acrobat 9.0 and earlier, allows remote attackers to execute arbitrary code via a crafted PDF document, related to a non-JavaScript function call and possibly an embedded JBIG2 image stream, as exploited in the wild in February 2009 by Trojan.Pidief.E.

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

References:

* MILWORM: 8090

<http://www.milw0rm.com/exploits/8090>

* MILWORM: 8099

<http://www.milw0rm.com/exploits/8099>

* MISC:

<http://isc.sans.org/diary.html?n&storyid=5902>

* MISC:

<http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20090219>

* MISC:

http://www.symantec.com/security_response/writeup.jsp?docid=2009-021212-5523-99&tabid=2

* CONFIRM:

<http://www.adobe.com/support/security/advisories/apsa09-01.html>

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb09-04.html>

* GENTOO: GLSA-200904-17

<http://security.gentoo.org/glsa/glsa-200904-17.xml>

* REDHAT: RHSA-2009:0376
<http://www.redhat.com/support/errata/RHSA-2009-0376.html>
* SUNALERT: 256788
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-256788-1>
* SUSE: SUSE-SA:2009:014
<http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00005.html>
* SUSE: SUSE-SR:2009:009
<http://lists.opensuse.org/opensuse-security-announce/2009-04/msg00010.html>
* CERT: TA09-051A
<http://www.us-cert.gov/cas/techalerts/TA09-051A.html>
* CERT-VN: VU#905281
<http://www.kb.cert.org/vuls/id/905281>
* BID: 33751
<http://www.securityfocus.com/bid/33751>
* FRSIRT: ADV-2009-0472
<http://www.frsirt.com/english/advisories/2009/0472>
* OSVDB: 52073
<http://osvdb.org/52073>
* OVAL: oval:org.mitre.oval:def:5697
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5697>
* SECTRACK: 1021739
<http://www.securitytracker.com/id?1021739>
* SECUNIA: 33901
<http://secunia.com/advisories/33901>
* SECUNIA: 34392
<http://secunia.com/advisories/34392>
* SECUNIA: 34490
<http://secunia.com/advisories/34490>
* SECUNIA: 34706
<http://secunia.com/advisories/34706>
* SECUNIA: 34790
<http://secunia.com/advisories/34790>
* VUPEN: ADV-2009-1019
<http://www.vupen.com/english/advisories/2009/1019>
* XF: adobe-acrobat-reader-image-bo(48825)
<http://xforce.iss.net/xforce/xfdb/48825>

CVE Reference:

CVE-2009-0658 (cve.mitre.org, nvd.nist.gov)

● 14507 Adobe Acrobat / Reader crafted argument to the getlcon method of a Collab object stack based buffer overflow Vulnerability (Remote File Checking)

Stack-based buffer overflow in Adobe Reader and Adobe Acrobat 9 before 9.1, 8 before 8.1.3, and 7 before 7.1.1 allows remote attackers to execute arbitrary code via a crafted argument to the getlcon method of a Collab object, a different vulnerability than CVE-2009-0658.

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

References:

* BUGTRAQ: 20090324 ZDI-09-014: Adobe Acrobat getlcon() Stack Overflow Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/502116/100/0/threaded>
* MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-09-014>
* CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb09-04.html>
* GENTOO: GLSA-200904-17
<http://security.gentoo.org/glsa/glsa-200904-17.xml>
* SUNALERT: 256788
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-256788-1>
* SUSE: SUSE-SA:2009:014
<http://lists.opensuse.org/opensuse-security-announce/2009-03/msg00005.html>
* SUSE: SUSE-SR:2009:009
<http://lists.opensuse.org/opensuse-security-announce/2009-04/msg00010.html>
* BID: 34169
<http://www.securityfocus.com/bid/34169>
* SECTRACK: 1021861
<http://www.securitytracker.com/id?1021861>
* SECUNIA: 34490

<http://secunia.com/advisories/34490>

* SECUNIA: 34706

<http://secunia.com/advisories/34706>

* SECUNIA: 34790

<http://secunia.com/advisories/34790>

* VUPEN: ADV-2009-0770

<http://www.vupen.com/english/advisories/2009/0770>

* VUPEN: ADV-2009-1019

<http://www.vupen.com/english/advisories/2009/1019>

* XF: adobe-undefined-javascript-code-execution(49312)

<http://xforce.iss.net/xforce/xfdb/49312>

CVE Reference:

CVE-2009-0927 (cve.mitre.org, nvd.nist.gov)

• 18388 Microsoft Office PowerPoint Heap Corruption Vulnerability (CVE-2009-1130) (MS09-017/967340) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

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

References:

* BUGTRAQ: 20090512 ZDI-09-020: Microsoft Office PowerPoint Notes Container Heap Overflow Vulnerability

<http://www.securityfocus.com/archive/1/503454>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-09-020/>

* MS: MS09-017

<http://www.microsoft.com/technet/security/Bulletin/MS09-017.msp>

* CERT: TA09-132A

<http://www.us-cert.gov/cas/techalerts/TA09-132A.html>

* BID: 34840

<http://www.securityfocus.com/bid/34840>

* SECTRACK: 1022205

<http://www.securitytracker.com/id?1022205>

* SECUNIA: 32428

<http://secunia.com/advisories/32428>

* VUPEN: ADV-2009-1290

<http://www.vupen.com/english/advisories/2009/1290>

CVE Reference:

CVE-2009-1130 (cve.mitre.org, nvd.nist.gov)

• 18389 Microsoft Office PowerPoint Data Out of Bounds Vulnerability (CVE-2009-1131) (MS09-017/967340) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

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

References:

* BUGTRAQ: 20090512 Secunia Research: Microsoft PowerPoint Atom Parsing Buffer Overflows

<http://www.securityfocus.com/archive/1/503451>

* MISC:

http://secunia.com/secunia_research/2008-46/

* MS: MS09-017

<http://www.microsoft.com/technet/security/Bulletin/MS09-017.msp>

* CERT: TA09-132A

<http://www.us-cert.gov/cas/techalerts/TA09-132A.html>

* BID: 34841

<http://www.securityfocus.com/bid/34841>

* OSVDB: 54393

<http://osvdb.org/54393>

* SECTRACK: 1022205

<http://www.securitytracker.com/id?1022205>

* SECUNIA: 32428
<http://secunia.com/advisories/32428>
* VUPEN: ADV-2009-1290
<http://www.vupen.com/english/advisories/2009/1290>

CVE Reference:

CVE-2009-1131 (cve.mitre.org, nvd.nist.gov)

● **18390 Microsoft Office PowerPoint Legacy File Format Vulnerability (CVE-2009-1137) (MS09-017/967340) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

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

References:

* MS: MS09-017
<http://www.microsoft.com/technet/security/Bulletin/MS09-017.msp>
* CERT: TA09-132A
<http://www.us-cert.gov/cas/techalerts/TA09-132A.html>
* BID: 34876
<http://www.securityfocus.com/bid/34876>
* OSVDB: 54381
<http://osvdb.org/54381>
* SECTRACK: 1022205
<http://www.securitytracker.com/id?1022205>
* SECUNIA: 32428
<http://secunia.com/advisories/32428>
* VUPEN: ADV-2009-1290
<http://www.vupen.com/english/advisories/2009/1290>
* XF: powerpoint-sounddata-code-execution(50425)
<http://xforce.iss.net/xforce/xfdb/50425>

CVE Reference:

CVE-2009-1137 (cve.mitre.org, nvd.nist.gov)

● **18391 Wireshark PROFINET dissector format string overflow Vulnerability (Remote File Checking)**

A format string vulnerability in the PROFINET/DCP (PN-DCP) dissector in Wireshark 1.0.6 and earlier allows remote attackers to execute arbitrary code via a PN-DCP packet with format string specifiers in the station name.

The vulnerability is reported in versions 0.99.6 to 1.0.6.

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

References:

* BUGTRAQ: 20090417 rPSA-2009-0062-1 tshark wireshark
<http://www.securityfocus.com/archive/1/archive/1/502745/100/0/threaded>
* MILWORM: 8308
<http://www.milworm.com/exploits/8308>
* CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2009-02.html>
* CONFIRM:
<http://wiki.rpath.com/Advisories:rPSA-2009-0062>
* DEBIAN: DSA-1785
<http://www.debian.org/security/2009/dsa-1785>
* FEDORA: FEDORA-2009-3599
<https://www.redhat.com/archives/fedora-package-announce/2009-May/msg00675.html>
* MANDRIVA: MDVSA-2009:088
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:088>
* BID: 34291
<http://www.securityfocus.com/bid/34291>
* SECUNIA: 34542
<http://secunia.com/advisories/34542>
* SECUNIA: 34778
<http://secunia.com/advisories/34778>
* SECUNIA: 34970

<http://secunia.com/advisories/34970>

* SECUNIA: 35133

<http://secunia.com/advisories/35133>

* XF: wireshark-pndcp-format-string(49512)

<http://xforce.iss.net/xforce/xfdb/49512>

CVE Reference:

CVE-2009-1210 (cve.mitre.org, nvd.nist.gov)

• 18392 Wireshark LDAP dissector Denial of Service Vulnerability (CVE-2009-1267) (Remote File Checking)

Unspecified vulnerability in the LDAP dissector in Wireshark 0.99.2 through 1.0.6, when running on Windows, allows remote attackers to cause a denial of service (crash) via unknown attack vectors.

The vulnerability is reported in versions 0.99.2 to 1.0.6.

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

References:

* BUGTRAQ: 20090417 rPSA-2009-0062-1 tshark wireshark

<http://www.securityfocus.com/archive/1/archive/1/502745/100/0/threaded>

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2009-02.html>

* CONFIRM:

<http://wiki.rpath.com/Advisories:rPSA-2009-0062>

* BID: 34457

<http://www.securityfocus.com/bid/34457>

* SECTRACK: 1022027

<http://www.securitytracker.com/id?1022027>

* SECUNIA: 34778

<http://secunia.com/advisories/34778>

* XF: wireshark-ldap-home-dos(49814)

<http://xforce.iss.net/xforce/xfdb/49814>

CVE Reference:

CVE-2009-1267 (cve.mitre.org, nvd.nist.gov)

• 18393 Wireshark Check Point High-Availability Protocol (CPHAP) dissector Denial of Service Vulnerability (Remote File Checking)

The Check Point High-Availability Protocol (CPHAP) dissector in Wireshark 0.9.6 through 1.0.6 allows remote attackers to cause a denial of service (crash) via a crafted FWHA_MY_STATE packet.

The vulnerability is reported in versions 0.9.6 to 1.0.6.

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

References:

* BUGTRAQ: 20090417 rPSA-2009-0062-1 tshark wireshark

<http://www.securityfocus.com/archive/1/archive/1/502745/100/0/threaded>

* MISC:

https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=3269

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2009-02.html>

* CONFIRM:

<http://wiki.rpath.com/Advisories:rPSA-2009-0062>

* DEBIAN: DSA-1785

<http://www.debian.org/security/2009/dsa-1785>

* FEDORA: FEDORA-2009-3599

<https://www.redhat.com/archives/fedora-package-announce/2009-May/msg00675.html>

* MANDRIVA: MDVSA-2009:088

<http://www.mandriva.com/security/advisories?name=MDVSA-2009:088>

* BID: 34457

<http://www.securityfocus.com/bid/34457>

* SECTRACK: 1022027

<http://www.securitytracker.com/id?1022027>

* SECUNIA: 34778

<http://secunia.com/advisories/34778>

* SECUNIA: 34970
<http://secunia.com/advisories/34970>
* SECUNIA: 35133
<http://secunia.com/advisories/35133>
* XF: wireshark-cphap-dos(49815)
<http://xforce.iss.net/xforce/xfdb/49815>

CVE Reference:

CVE-2009-1268 (cve.mitre.org, nvd.nist.gov)

• 18394 Wireshark Tektronix .rf5 dissector Denial of Service Vulnerability (Remote File Checking)

An unspecified vulnerability in Wireshark 0.99.6 through 1.0.6 allows remote attackers to cause a denial of service (crash) via a crafted Tektronix .rf5 file.

The vulnerability is reported in versions 0.99.6 to 1.0.6.

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

References:

* BUGTRAQ: 20090417 rPSA-2009-0062-1 tshark wireshark
<http://www.securityfocus.com/archive/1/archive/1/502745/100/0/threaded>
* CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2009-02.html>
* CONFIRM:
<http://wiki.rpath.com/Advisories:rPSA-2009-0062>
* DEBIAN: DSA-1785
<http://www.debian.org/security/2009/dsa-1785>
* FEDORA: FEDORA-2009-3599
<https://www.redhat.com/archives/fedora-package-announce/2009-May/msg00675.html>
* MANDRIVA: MDVSA-2009:088
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:088>
* BID: 34457
<http://www.securityfocus.com/bid/34457>
* SECTRACK: 1022027
<http://www.securitytracker.com/id?1022027>
* SECUNIA: 34778
<http://secunia.com/advisories/34778>
* SECUNIA: 34970
<http://secunia.com/advisories/34970>
* SECUNIA: 35133
<http://secunia.com/advisories/35133>
* XF: wireshark-rf5file-dos(49816)
<http://xforce.iss.net/xforce/xfdb/49816>

CVE Reference:

CVE-2009-1269 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-1790 HP CVSS 2.0 Score = 4.3

Cross-site scripting (XSS) vulnerability in CGI RESCUE Trees before 2.11 allows remote attackers to inject arbitrary web script or HTML via unspecified parameters.

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

References:

BID: <http://www.securityfocus.com/bid/34999>
XF: <http://xforce.iss.net/xforce/xfdb/50579>
CONFIRM: <http://www.rescue.ne.jp/whatsnew/blog.cgi/permalink/20090512155247>
SECUNIA: <http://secunia.com/advisories/35123>
OSVDB: <http://osvdb.org/54545>

JVNDB: <http://jvndb.jvn.jp/en/contents/2009/JVNDB-2009-000028.html>

JVN: <http://jvn.jp/en/jp/JVN28521500/index.html>

CVE Reference: [CVE-2009-1790](#)

• **CVE-2009-1786 IBM CVSS 2.0 Score = 6.9**

The malloc subsystem in libc in IBM AIX 5.3 and 6.1 allows local users to create or overwrite arbitrary files via a symlink attack on the log file associated with the MALLOCDDEBUG environment variable.

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

References:

SECTRAK: <http://securitytracker.com/id?1022261>

CONFIRM: http://aix.software.ibm.com/aix/efixes/security/libc_advisory.asc

XF: <http://xforce.iss.net/xforce/xfdb/50636>

VUPEN: <http://www.vupen.com/english/advisories/2009/1380>

BID: <http://www.securityfocus.com/bid/35034>

OSVDB: <http://www.osvdb.org/54617>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ50517>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ50500>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ50447>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ50445>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ50139>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ50129>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ50121>

SECUNIA: <http://secunia.com/advisories/35146>

IDEFENSE: <http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=802>

CVE Reference: [CVE-2009-1786](#)

• **CVE-2009-1636 Novell CVSS 2.0 Score = 10.0**

Multiple buffer overflows in the Internet Agent (aka GWIA) component in Novell GroupWise 7.x before 7.03 HP3 and 8.x before 8.0 HP2 allow remote attackers to execute arbitrary code via (1) a crafted e-mail address in an SMTP session or (2) an SMTP command.

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

References:

MISC: https://bugzilla.novell.com/show_bug.cgi?id=482914

MISC: https://bugzilla.novell.com/show_bug.cgi?id=478892

MISC:

http://www.vupen.com/exploits/Novell_GroupWise_GWIA_SSMTP_Command_Remote_Buffer_Overflow_PoC_Exploit_139

MISC:

http://www.vupen.com/exploits/Novell_GroupWise_GWIA_Email_Address_Remote_Buffer_Overflow_Exploit_1393141.ph

VUPEN: <http://www.vupen.com/english/advisories/2009/1393>

BID: <http://www.securityfocus.com/bid/35065>

BID: <http://www.securityfocus.com/bid/35064>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/503724/100/0/threaded>

CONFIRM: <http://www.novell.com/support/viewContent.do?externalId=7003273&sliceId=1>

CONFIRM: <http://www.novell.com/support/viewContent.do?externalId=7003272&sliceId=1>

SECUNIA: <http://secunia.com/advisories/35177>

CVE Reference: [CVE-2009-1636](#)

• **CVE-2008-3869 Sun CVSS 2.0 Score = 10.0**

Heap-based buffer overflow in sadmind in Sun Solaris 8 and 9 allows remote attackers to execute arbitrary code via a crafted RPC request, related to improper decoding of request parameters.

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

References:

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-66-259468-1>

CONFIRM: <http://sunsolve.sun.com/search/document.do?assetkey=1-21-116455-02-1>

BID: <http://www.securityfocus.com/bid/35083>

OSVDB: <http://www.osvdb.org/54663>

MISC: http://secunia.com/secunia_research/2008-45/

SECUNIA: <http://secunia.com/advisories/32473>

CVE Reference: [CVE-2008-3869](#)

• **CVE-2008-3870 Sun CVSS 2.0 Score = 10.0**

Integer overflow in sadmind in Sun Solaris 8 and 9 allows remote attackers to execute arbitrary code via a crafted RPC request that triggers a heap-based buffer overflow, related to improper memory allocation.

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

References:

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-66-259468-1>

CONFIRM: <http://sunsolve.sun.com/search/document.do?assetkey=1-21-116455-02-1>

BID: <http://www.securityfocus.com/bid/35083>

OSVDB: <http://www.osvdb.org/54668>

MISC: http://secunia.com/secunia_research/2008-47/

SECUNIA: <http://secunia.com/advisories/32473>

CVE Reference: [CVE-2008-3870](#)

• **CVE-2009-1634 Novell CVSS 2.0 Score = 7.5**

The WebAccess component in Novell GroupWise 7.x before 7.03 HP3 and 8.x before 8.0 HP2 does not properly implement session management mechanisms, which allows remote attackers to gain access to user accounts via unspecified vectors.

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

References:

MISC: https://bugzilla.novell.com/show_bug.cgi?id=472979

VUPEN: <http://www.vupen.com/english/advisories/2009/1393>

BID: <http://www.securityfocus.com/bid/35066>

CONFIRM: <http://www.novell.com/support/viewContent.do?externalId=7003266&sliceId=1>

SECUNIA: <http://secunia.com/advisories/35177>

CVE Reference: [CVE-2009-1634](#)

• **CVE-2009-1796 Sun CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in Sun Java System Portal Server 6.3.1, 7.1, and 7.2 allows remote attackers to inject arbitrary web script or HTML via vectors related to an error page.

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

References:

BID: <http://www.securityfocus.com/bid/35082>

SUNALERT: <http://sunsolve.sun.com/search/document.do?assetkey=1-66-256588-1>

CONFIRM: <http://sunsolve.sun.com/search/document.do?assetkey=1-21-118950-38-1>

CVE Reference: [CVE-2009-1796](#)

• **CVE-2009-0588 redhat CVSS 2.0 Score = 6.5**

agent/request/op.cgi in the Registration Authority (RA) component in Red Hat Certificate System (RHCS) 7.3 and Dogtag Certificate System allows remote authenticated users to approve certificate requests queued for arbitrary agent groups via a modified request ID field.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=484828

REDHAT: <http://www.redhat.com/support/errata/RHSA-2009-1065.html>

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=488706

BID: <http://www.securityfocus.com/bid/35104>

CVE Reference: [CVE-2009-0588](#)

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