

2011 Issue #25

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

[Apache Chunked Vulnerability Scanner](#) - The S4 Apache Chunked Vulnerability 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 Apache Chunked Encoding buffer overflow.

Download Here:

<http://www2.netvigilance.com/productdownloads?productname=apachechunkedvulnerabilityscanner>

This Week in Review

Breaches - its everyone's problem. UK person arrested may be LulzSec member. US guidelines for cyberwar laid out. Large Zeus spam campaign.

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

• Nine out of 10 businesses breached in the last year

Ninety percent of organizations have sustained at least one data breach in the past year, according to a survey released Wednesday by the Ponemon Institute and Juniper Networks. Even worse, the survey of 583 U.S. IT and IT security practitioners found that a majority of organizations have experienced multiple successful attacks against their networks.

Fifty-nine percent of respondents said their networks have been compromised at least two times in the past year. Just 10 percent said they have had no breaches.

Seventy-eight percent of those surveyed said there has been an increase in the frequency of attacks in the past year. Moreover, most respondents said attacks have become more severe and difficult to detect and contain. SC Magazine

Full Story :

http://www.scmagazineus.com/nine-out-of-10-businesses-breached-in-the-last-year/article/205888/?utm_source=feed

• **With Anonymous and LulzSec, is anyone believable?**

In a tweet, LulzSec denies that the arrested U.K. man was part of the hacker group.

For several months, hackers have been having a heyday taking down Web sites and leaking data from compromised servers with victims ranging from the CIA and U.S. Senate to Sony, Citigroup and the Turkish government. (A growing list of attacks is here).

A 19-year-old identified as Ryan Cleary was arrested Tuesday in the U.K. on hacking charges, but it's unclear whether he was involved with either of the two main hacker groups that have been taking responsibility for and organizing some of the attacks--Anonymous and LulzSec. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20073143-245/with-anonymous-and-lulzsec-is-anyone-believable/?part=rss&subj

• **Report: President lays out cyberwar guidelines**

President Barack Obama has developed guidelines for how the U.S. should respond to--and initiate--cyberattacks, the Associated Press is reporting.

Citing anonymous defense officials, the news service claims the guidelines include a wide range of cyberwar efforts to be employed by the U.S. during both peacetime and when conflicts are underway, including installing viruses on international computers and taking down a country's electrical grid.

According to the Associated Press, the guidelines also allow for defense officials to transmit code through another country's network to ensure the connection can be made. Though it wouldn't necessarily carry a dangerous payload at the time, that connection could be used in the future if an attack was authorized on the specific country. Cnet Security

Full Story :

http://news.cnet.com/8301-13506_3-20073314-17/president-lays-out-cyberwar-guidelines-report-says/?part=rss&subj

• **New Zeus emails cloaked as Fed, IRS messages**

Small and midsize organizations may want to take note: There is a particularly large Zeus spam campaign making the rounds.

The emails piggyback on two trusted names -- the Federal Reserve and the Internal Revenue Service -- to incite recipients to take unwise actions.

Researchers at Barracuda Labs first spotted the huge uptick in the malicious messages on Monday morning, when the emails were blocked before reaching some 120,000 users within 10 minutes. SC Magazine

Full Story :

http://www.scmagazineus.com/new-zeus-emails-cloaked-as-fed-irs-messages/article/205920/?utm_source=feedburner

New Vulnerabilities Tested in SecureScout

• **19351 Wireshark LDAP and SMB dissectors overflow Vulnerabilities (Remote File Checking)**

Multiple stack consumption vulnerabilities in the dissect_ms_compressed_string and dissect_msldap_string functions in Wireshark 1.0.x, 1.2.0 through 1.2.14, and 1.4.0 through 1.4.3 allow remote attackers to cause a denial of service (infinite recursion) via a crafted (1) SMB or (2) Connection-less LDAP (CLDAP) packet.

The vulnerability is reported in versions 1.0.x, 1.2.0 to 1.2.14 and 1.4.0 to 1.4.3.

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

References:

* CONFIRM:

<http://anonsvn.wireshark.org/viewvc?view=rev&revision=36029>

* CONFIRM:

<http://www.wireshark.org/docs/relnotes/wireshark-1.2.15.html>

* CONFIRM:

<http://www.wireshark.org/docs/relnotes/wireshark-1.4.4.html>

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2011-03.html>

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2011-04.html>

* CONFIRM:

https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=5717
* DEBIAN: DSA-2201
<http://www.debian.org/security/2011/dsa-2201>
* MANDRIVA: MDVSA-2011:044
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:044>
* REDHAT: RHSA-2011:0370
<http://www.redhat.com/support/errata/RHSA-2011-0370.html>
* REDHAT: RHSA-2011:0369
<http://www.redhat.com/support/errata/RHSA-2011-0369.html>
* SUSE: openSUSE-SU-2011:0347
<https://hermes.opensuse.org/messages/8086844>
* SECTRACK: 1025148
<http://www.securitytracker.com/id?1025148>
* SECUNIA: 43821
<http://secunia.com/advisories/43821>
* SECUNIA: 43795
<http://secunia.com/advisories/43795>
* SECUNIA: 44169
<http://secunia.com/advisories/44169>
* VUPEN: ADV-2011-0719
<http://www.vupen.com/english/advisories/2011/0719>
* VUPEN: ADV-2011-0622
<http://www.vupen.com/english/advisories/2011/0622>
* VUPEN: ADV-2011-0747
<http://www.vupen.com/english/advisories/2011/0747>

CVE Reference:

CVE-2011-1140 (cve.mitre.org, nvd.nist.gov)

• 19352 Wireshark large LDAP Filter strings denial of service Vulnerability (Remote File Checking)

epan/dissectors/packet-ldap.c in Wireshark 1.0.x, 1.2.0 through 1.2.14, and 1.4.0 through 1.4.3 allows remote attackers to cause a denial of service (memory consumption) via (1) a long LDAP filter string or (2) an LDAP filter string containing many elements.

The vulnerability is reported in versions 1.0.x, 1.2.0 to 1.2.14 and 1.4.0 to 1.4.3.

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

References:

* CONFIRM:
<http://anonsvn.wireshark.org/viewvc?view=rev&revision=36101>
* CONFIRM:
<http://www.wireshark.org/docs/relnotes/wireshark-1.2.15.html>
* CONFIRM:
<http://www.wireshark.org/docs/relnotes/wireshark-1.4.4.html>
* CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2011-03.html>
* CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2011-04.html>
* CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=5732
* DEBIAN: DSA-2201
<http://www.debian.org/security/2011/dsa-2201>
* MANDRIVA: MDVSA-2011:044
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:044>
* REDHAT: RHSA-2011:0370
<http://www.redhat.com/support/errata/RHSA-2011-0370.html>
* REDHAT: RHSA-2011:0369
<http://www.redhat.com/support/errata/RHSA-2011-0369.html>
* SECTRACK: 1025148
<http://www.securitytracker.com/id?1025148>
* SECUNIA: 43821
<http://secunia.com/advisories/43821>
* SECUNIA: 43795
<http://secunia.com/advisories/43795>
* VUPEN: ADV-2011-0719
<http://www.vupen.com/english/advisories/2011/0719>
* VUPEN: ADV-2011-0622

<http://www.vupen.com/english/advisories/2011/0622>

* VUPEN: ADV-2011-0747

<http://www.vupen.com/english/advisories/2011/0747>

CVE Reference:

CVE-2011-1141 (cve.mitre.org, nvd.nist.gov)

• 19353 Wireshark malformed 6LoWPAN packet denial of service Vulnerability (Remote File Checking)

Off-by-one error in the dissect_6lowpan_iphc function in packet-6lowpan.c in Wireshark 1.4.0 through 1.4.3 on 32-bit platforms allows remote attackers to cause a denial of service (application crash) via a malformed 6LoWPAN IPv6 packet.

The vulnerability is reported in versions 1.4.0 to 1.4.3.

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

References:

* CONFIRM:

<http://anonsvn.wireshark.org/viewvc?view=rev&revision=36036>

* CONFIRM:

<http://www.wireshark.org/docs/relnotes/wireshark-1.4.4.html>

* CONFIRM:

<http://www.wireshark.org/security/wmpa-sec-2011-04.html>

* CONFIRM:

https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=5722

* SUSE: openSUSE-SU-2011:0347

<https://hermes.opensuse.org/messages/8086844>

* BID: 46636

<http://www.securityfocus.com/bid/46636>

* SECTRACK: 1025148

<http://www.securitytracker.com/id?1025148>

* SECUNIA: 44169

<http://secunia.com/advisories/44169>

* XF: wireshark6lowpan-bo(65783)

<http://xforce.iss.net/xforce/xfdb/65783>

CVE Reference:

CVE-2011-1138 (cve.mitre.org, nvd.nist.gov)

• 19364 Adobe Flash Player bounds checking Vulnerability (CVE-2011-0626) (Remote File Checking)

Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors, related to a "bounds checking" issue, a different vulnerability than CVE-2011-0623, CVE-2011-0624, and CVE-2011-0625.

Adobe Flash Player version 10.3.181.14 resolves the issue.

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

References:

* BID: 47814

<http://www.securityfocus.com/bid/47814>

* SECTRACK: 1025533

<http://securitytracker.com/id/1025533>

* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb11-12.html>

CVE Reference:

CVE-2011-0626 (cve.mitre.org, nvd.nist.gov)

• 19365 Adobe Flash Player memory corruption Vulnerability (CVE-2011-0627) (Remote File Checking)

Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content, as possibly exploited in the wild in May 2011 by a Microsoft Office document with an embedded .swf file.

Adobe Flash Player version 10.3.181.14 resolves the issue.

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

References:

- * BID: 47810
<http://www.securityfocus.com/bid/47810>
- * SECTRACK: 1025533
<http://securitytracker.com/id/1025533>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-12.html>

CVE Reference:

CVE-2011-0627 (cve.mitre.org, nvd.nist.gov)

• **19366 Adobe Flash Player integer overflow Vulnerability (CVE-2011-0628) (Remote File Checking)**

Integer overflow in Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows remote attackers to execute arbitrary code via ActionScript that improperly handles a long array object.

Adobe Flash Player version 10.3.181.14 resolves the issue.

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

References:

- * BID: 47810
<http://www.securityfocus.com/bid/47810>
- * SECTRACK: 1025533
<http://securitytracker.com/id/1025533>
- * IDEFENSE: 20110524 Adobe Flash Player ActionScript Integer Overflow Vulnerability
<http://labs.odefense.com/intelligence/vulnerabilities/display.php?id=908>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-12.html>
- * BID: 47961
<http://www.securityfocus.com/bid/47961>
- * XF: flash-player-overflow(67638)
<http://xforce.iss.net/xfdb/67638>

CVE Reference:

CVE-2011-0628 (cve.mitre.org, nvd.nist.gov)

• **19367 Adobe Flash Player universal cross-site scripting Vulnerability (CVE-2011-2107) (Remote File Checking)**

Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 10.3.181.22 on Windows, Mac OS X, Linux, and Solaris, and 10.3.185.22 and earlier on Android, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, related to a "universal cross-site scripting vulnerability."

Adobe Flash Player version 10.3.181.22 resolves the issue.

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

References:

- * BID: 48107
<http://www.securityfocus.com/bid/48107>
- * SECTRACK: 1025603
<http://securitytracker.com/id/1025603>
- * CONFIRM:
<http://www.adobe.com/support/security/bulletins/apsb11-13.html>

CVE Reference:

CVE-2011-2107 (cve.mitre.org, nvd.nist.gov)

• **19378 Selection Object Memory Corruption Vulnerability (MS11-050/2530548) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. The vulnerability may corrupt memory in such a way that an attacker could

execute arbitrary code in the context of the logged-on user.

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

References:

- * MS: MS11-050
<http://www.microsoft.com/technet/security/Bulletin/MS11-050.msp>
- * BID: 48210
<http://www.securityfocus.com/bid/48210>
- * SECTRACK: 1025649
<http://securitytracker.com/id/1025649>

CVE Reference:

CVE-2011-1261 (cve.mitre.org, nvd.nist.gov)

• 19379 HTTP Redirect Memory Corruption Vulnerability (MS11-050/2530548) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. The vulnerability may corrupt memory in such a way that an attacker could execute arbitrary code in the context of the logged-on user.

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

References:

- * MS: MS11-050
<http://www.microsoft.com/technet/security/Bulletin/MS11-050.msp>
- * BID: 48211
<http://www.securityfocus.com/bid/48211>
- * SECTRACK: 1025649
<http://securitytracker.com/id/1025649>

CVE Reference:

CVE-2011-1262 (cve.mitre.org, nvd.nist.gov)

• 19380 SMB Response Parsing Vulnerability (MS11-043/2536276) (Remote File Checking)

An unauthenticated remote code execution vulnerability exists in the way that the Microsoft Server Message Block (SMB) client implementation handles specially crafted SMB responses. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted SMB response to a client-initiated SMB request. An attacker who successfully exploited this vulnerability could execute arbitrary code and take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

- * BID: 48184
<http://www.securityfocus.com/bid/48184>
- * SECTRACK: 1025640
<http://www.securitytracker.com/id/1025640>
- * MS: MS11-043
<http://www.microsoft.com/technet/security/Bulletin/MS11-043.msp>

CVE Reference:

CVE-2011-1268 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-1173 Linux CVSS 2.0 Score = 5.0

The econet_sendmsg function in net/econet/af_econet.c in the Linux kernel before 2.6.39 on the x86_64 platform allows remote attackers to obtain potentially sensitive information from kernel stack memory by reading uninitialized data in the ah field of an Acorn Universal Networking (AUN) packet.

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

References:

MLIST: <http://www.openwall.com/lists/oss-security/2011/03/21/4>

MLIST: <http://www.openwall.com/lists/oss-security/2011/03/21/1>

MLIST: <http://www.openwall.com/lists/oss-security/2011/03/18/15>

MLIST: <http://marc.info/?l=linux-netdev&m=130036203528021&w=2>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=67c5c6cb8129c595f21e88254a3fc6b3b841ae8e>

MISC: https://bugzilla.redhat.com/show_bug.cgi?id=591815#c14

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.39>

CVE Reference: [CVE-2011-1173](#)

• **CVE-2011-2534 Linux CVSS 2.0 Score = 4.0**

Buffer overflow in the clusterip_proc_write function in net/ipv4/netfilter/ipt_CLUSTERIP.c in the Linux kernel before 2.6.39 might allow local users to cause a denial of service or have unspecified other impact via a crafted write operation, related to string data that lacks a terminating '\0' character.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=689337

MLIST: <http://www.openwall.com/lists/oss-security/2011/03/21/4>

MLIST: <http://www.openwall.com/lists/oss-security/2011/03/21/1>

MLIST: <http://www.openwall.com/lists/oss-security/2011/03/18/15>

MLIST: <http://marc.info/?l=netfilter-devel&m=130036157327564&w=2>

MLIST: <http://marc.info/?l=netfilter&m=129978077509888&w=2>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=961ed183a9fd080cf306c659b8736007e44065a5>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.39>

CVE Reference: [CVE-2011-2534](#)

• **CVE-2011-1170 Linux CVSS 2.0 Score = 2.1**

net/ipv4/netfilter/arp_tables.c in the IPv4 implementation in the Linux kernel before 2.6.39 does not place the expected '\0' character at the end of string data in the values of certain structure members, which allows local users to obtain potentially sensitive information from kernel memory by leveraging the CAP_NET_ADMIN capability to issue a crafted request, and then reading the argument to the resulting modprobe process.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=689321

MLIST: <http://www.openwall.com/lists/oss-security/2011/03/21/4>

MLIST: <http://www.openwall.com/lists/oss-security/2011/03/21/1>

MLIST: <http://www.openwall.com/lists/oss-security/2011/03/18/15>

MLIST: <http://marc.info/?l=netfilter-devel&m=129978081009955&w=2>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=42eab94fff18cb1091d3501cd284d6bd6cc9c143>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.39>

CVE Reference: [CVE-2011-1170](#)

• **CVE-2011-1172 Linux CVSS 2.0 Score = 2.1**

net/ipv6/netfilter/ip6_tables.c in the IPv6 implementation in the Linux kernel before 2.6.39 does not place the expected '\0' character at the end of string data in the values of certain structure members, which allows local users to obtain potentially sensitive information from kernel memory by leveraging the CAP_NET_ADMIN capability to issue a crafted request, and then reading the argument to the resulting modprobe process.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=689345

MLIST: <http://www.openwall.com/lists/oss-security/2011/03/21/4>

MLIST: <http://www.openwall.com/lists/oss-security/2011/03/21/1>

MLIST: <http://www.openwall.com/lists/oss-security/2011/03/18/15>

MLIST: <http://marc.info/?l=linux-kernel&m=129978086410061&w=2>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=6a8ab060779779de8aea92ce3337ca348f973f54>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.39>

CVE Reference: [CVE-2011-1172](#)

• **CVE-2011-1171 Linux CVSS 2.0 Score = 2.1**

net/ipv4/netfilter/ip_tables.c in the IPv4 implementation in the Linux kernel before 2.6.39 does not place the expected '\0' character at the end of string data in the values of certain structure members, which allows local users to obtain potentially sensitive information from kernel memory by leveraging the CAP_NET_ADMIN capability to issue a crafted request, and then reading the argument to the resulting modprobe process.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=689327

MLIST: <http://www.openwall.com/lists/oss-security/2011/03/21/4>

MLIST: <http://www.openwall.com/lists/oss-security/2011/03/21/1>

MLIST: <http://www.openwall.com/lists/oss-security/2011/03/18/15>

MLIST: <http://marc.info/?l=linux-kernel&m=129978077609894&w=2>

CONFIRM:

<http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=78b79876761b86653df89c48a7010b5cbd41a84a>

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.39>

CVE Reference: [CVE-2011-1171](#)

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