

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

New attack on Sony. Cyberwar facet of regular war? RSA data used in breach. Tennessee makes sharing login information illegal.

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

• Hacker group raids Sony Pictures in latest breach

Fresh off the successful infiltration and defacement of the PBS website, the hacktivist collective known as LulzSec said Thursday that it has compromised the personal information of more than one million users of SonyPictures.com.

The revelation deals another devastating blow to a company already reeling from a number of recent intrusions, most notably the breach of the Sony PlayStation Network, one of the largest reported data theft incidents of all time.

In a news release, LulzSec said its members exploited a common SQL injection vulnerability to gain access to internal Sony networks and websites. The hack yielded the passwords, email addresses, home addresses, birth dates and other account information belonging to more than one million users. The intruders posted some of the booty on their newly created website. SC Magazine

Full Story :

http://www.scmagazineus.com/hacker-group-raids-sony-pictures-in-latest-breach/article/204379/?utm_source=feedb

• U.S., U.K. see cyberwar as facet of regular war

Symantec's report includes a graphical representation of Stuxnet infections linked to organizations in Iran.

(Credit: Symantec) Reports from the United States and United Kingdom military this week indicate those organizations are more comfortable voicing an idea I find blindingly obvious: cyberwar is war.

First came news yesterday in the Guardian that the U.K. is developing offensive weapons that could be used in attacks on computing systems as "an integral part of the country's armory." Cnet Security

Full Story :

http://news.cnet.com/8301-30685_3-20067465-264.html?part=rss&subj=news&tag=2547-1_3-0-20

• Report: Data stolen in RSA breach used to target defense contractor

Defense contractor L-3 Communications told employees that attackers used SecurID information stolen from RSA in March to target L-3, according to a report.

"L-3 Communications has been actively targeted with penetration attacks leveraging the compromised information," said an April 6 e-mail from an executive at L-3's Stratus Group to the group's 5,000 workers, which Wired published yesterday after receiving it from an unidentified source. The source reportedly said SecurID is used for access to an unclassified corporate network, but not classified networks.

It is unclear if the attack was successful. "Protecting our network is a top priority, and we have a robust set of protocols in place to ensure sensitive information is safeguarded. We have gotten to the bottom of the issue," L-3 spokeswoman Jennifer Barton told Kevin Poulsen at Wired, declining to comment further. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20068051-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• Feds investigate alleged attacks on Gmail accounts

The U.S. government is investigating reports from Google that hackers attempted to break into the Gmail accounts of senior government officials but at this point doesn't believe any accounts were actually breached.

"Speaking on behalf of the U.S. government, we're looking into these reports and seeking to gather the facts," Caitlin Hayden, deputy spokesperson for the National Security Council, told CNET today. "We have no reason to believe that any official U.S. government e-mail accounts were accessed."

The FBI is taking the lead on the investigation, according to Hayden, "as part of an interagency mechanism that comes together to focus on these types of incidents when they occur." Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20068229-83/feds-investigate-alleged-attacks-on-gmail-accounts/?part=rss&subj=

New Vulnerabilities Tested in SecureScout

• 19341 Wireshark DLL hijacking Vulnerability (Remote File Checking)

Untrusted search path vulnerability in Wireshark 0.8.4 through 1.0.15 and 1.2.0 through 1.2.10 allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse airpcap.dll, and possibly other DLLs, that is located in the same folder as a file that automatically launches Wireshark.

The vulnerability is reported in versions 0.8.4 through 1.0.15 and 1.2.0 through 1.2.10.

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

References:

* EXPLOIT-DB: 14721

<http://www.exploit-db.com/exploits/14721/>

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2010-09.html>

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2010-10.html>

* SECUNIA: 41064

<http://secunia.com/advisories/41064>

* VUPEN: ADV-2010-2165

<http://www.vupen.com/english/advisories/2010/2165>

* VUPEN: ADV-2010-2243

<http://www.vupen.com/english/advisories/2010/2243>

CVE Reference:

CVE-2010-3133 (cve.mitre.org, nvd.nist.gov)

• 19342 Wireshark ASN.1 BER dissector overflow Vulnerability (Remote File Checking)

Stack consumption vulnerability in the dissect_ber_unknown function in epan/dissectors/packet-ber.c in the BER dissector in Wireshark 1.4.x before 1.4.1 and 1.2.x before 1.2.12 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a long string in an unknown ASN.1/BER encoded packet, as demonstrated using SNMP.

The vulnerability is reported in versions 1.2.0 through 1.2.11, and 1.4.0.

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

References:

- * BUGTRAQ: 20100913 Wireshark 1.4.0 Malformed SNMP V1 Packet Denial of Service
<http://archives.neohapsis.com/archives/bugtrag/2010-09/0088.html>
- * MLIST: [oss-security] 20101001 Re: CVE requests: Poppler, Quassel, Pyfribidi, Overkill, DocUtils, FireGPG, Wireshark
<http://www.openwall.com/lists/oss-security/2010/10/01/10>
- * MLIST: [oss-security] 20101011 Re: CVE requests: Poppler, Quassel, Pyfribidi, Overkill, DocUtils, FireGPG, Wireshark
<http://www.openwall.com/lists/oss-security/2010/10/12/1>
- * MISC:
<http://xorl.wordpress.com/2010/10/15/cve-2010-3445-wireshark-asn-1-ber-stack-overflow/>
- * CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=5230
- * CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2010-3445
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2010-12.html>
- * CONFIRM:
http://blogs.sun.com/security/entry/resource_management_errors_vulnerability_in
- * DEBIAN: DSA-2127
<http://www.debian.org/security/2010/dsa-2127>
- * MANDRIVA: MDVSA-2010:200
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:200>
- * REDHAT: RHSA-2010:0924
<http://www.redhat.com/support/errata/RHSA-2010-0924.html>
- * REDHAT: RHSA-2011:0370
<http://www.redhat.com/support/errata/RHSA-2011-0370.html>
- * SUSE: SUSE-SR:2011:001
<http://lists.opensuse.org/opensuse-security-announce/2011-01/msg00003.html>
- * SUSE: SUSE-SR:2011:002
<http://lists.opensuse.org/opensuse-security-announce/2011-01/msg00006.html>
- * BID: 43197
<http://www.securityfocus.com/bid/43197>
- * SECUNIA: 42392
<http://secunia.com/advisories/42392>
- * SECUNIA: 42411
<http://secunia.com/advisories/42411>
- * SECUNIA: 42877
<http://secunia.com/advisories/42877>
- * SECUNIA: 43068
<http://secunia.com/advisories/43068>
- * SECUNIA: 43821
<http://secunia.com/advisories/43821>
- * VUPEN: ADV-2010-3067
<http://www.vupen.com/english/advisories/2010/3067>
- * VUPEN: ADV-2010-3093
<http://www.vupen.com/english/advisories/2010/3093>
- * VUPEN: ADV-2011-0076
<http://www.vupen.com/english/advisories/2011/0076>
- * VUPEN: ADV-2011-0212
<http://www.vupen.com/english/advisories/2011/0212>
- * VUPEN: ADV-2011-0404
<http://www.vupen.com/english/advisories/2011/0404>

* VUPEN: ADV-2011-0719
<http://www.vupen.com/english/advisories/2011/0719>
* BID: 43923
<http://www.securityfocus.com/bid/43923>

CVE Reference:

CVE-2010-3445 (cve.mitre.org, nvd.nist.gov)

• 19343 Wireshark LDSS dissector overflow Vulnerability (Remote File Checking)

Heap-based buffer overflow in the dissect_ldss_transfer function (epan/dissectors/packet-ldss.c) in the LDSS dissector in Wireshark 1.2.0 through 1.2.12 and 1.4.0 through 1.4.1 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via an LDSS packet with a long digest line that triggers memory corruption.

The vulnerability is reported in versions 1.2.0 to 1.2.12 and 1.4.0 to 1.4.1

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

References:

* EXPLOIT-DB: 15676
<http://www.exploit-db.com/exploits/15676>
* CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2010-14.html>
* CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=5318
* CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2010-13.html>
* CONFIRM:
http://blogs.sun.com/security/entry/buffer_overflow_vulnerability_in_wireshark
* MANDRIVA: MDVSA-2010:242
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:242>
* REDHAT: RHSA-2010:0924
<http://www.redhat.com/support/errata/RHSA-2010-0924.html>
* SUSE: SUSE-SR:2011:001
<http://lists.opensuse.org/opensuse-security-announce/2011-01/msg00003.html>
* SUSE: SUSE-SR:2011:002
<http://lists.opensuse.org/opensuse-security-announce/2011-01/msg00006.html>
* BID: 44987
<http://www.securityfocus.com/bid/44987>
* OSVDB: 69354
<http://osvdb.org/69354>
* SECTRACK: 1024762
<http://www.securitytracker.com/id?1024762>
* SECUNIA: 42290
<http://secunia.com/advisories/42290>
* SECUNIA: 42411
<http://secunia.com/advisories/42411>
* SECUNIA: 42877
<http://secunia.com/advisories/42877>
* SECUNIA: 43068
<http://secunia.com/advisories/43068>
* VUPEN: ADV-2010-3038
<http://www.vupen.com/english/advisories/2010/3038>
* VUPEN: ADV-2010-3068
<http://www.vupen.com/english/advisories/2010/3068>
* VUPEN: ADV-2010-3093
<http://www.vupen.com/english/advisories/2010/3093>
* VUPEN: ADV-2011-0076
<http://www.vupen.com/english/advisories/2011/0076>
* VUPEN: ADV-2011-0212
<http://www.vupen.com/english/advisories/2011/0212>
* VUPEN: ADV-2011-0404
<http://www.vupen.com/english/advisories/2011/0404>

CVE Reference:

CVE-2010-4300 (cve.mitre.org, nvd.nist.gov)

• 19344 Wireshark ZigBee ZCL dissector infinite loop Vulnerability (Remote File Checking)

epan/dissectors/packet-zbee-zcl.c in the ZigBee ZCL dissector in Wireshark 1.4.0 through 1.4.1 allows remote attackers to cause a denial of service (infinite loop) via a crafted ZCL packet, related to Discover Attributes.

The vulnerability is reported in versions 1.4.0 through 1.4.1.

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

References:

- * EXPLOIT-DB: 15973
<http://www.exploit-db.com/exploits/15973>
- * MISC:
<https://bugs.wireshark.org/bugzilla/attachment.cgi?id=5315&action=edit>
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2010-14.html>
- * CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=5303
- * SUSE: SUSE-SR:2011:001
<http://lists.opensuse.org/opensuse-security-announce/2011-01/msg00003.html>
- * SUSE: SUSE-SR:2011:002
<http://lists.opensuse.org/opensuse-security-announce/2011-01/msg00006.html>
- * BID: 44986
<http://www.securityfocus.com/bid/44986>
- * OSVDB: 69355
<http://osvdb.org/69355>
- * SECUNIA: 42290
<http://secunia.com/advisories/42290>
- * SECUNIA: 42877
<http://secunia.com/advisories/42877>
- * SECUNIA: 43068
<http://secunia.com/advisories/43068>
- * VUPEN: ADV-2010-3038
<http://www.vupen.com/english/advisories/2010/3038>
- * VUPEN: ADV-2011-0076
<http://www.vupen.com/english/advisories/2011/0076>
- * VUPEN: ADV-2011-0212
<http://www.vupen.com/english/advisories/2011/0212>

CVE Reference:

CVE-2010-4301 (cve.mitre.org, nvd.nist.gov)

• 19345 Wireshark MAC-LTE dissector overflow Vulnerability (Remote File Checking)

Buffer overflow in the MAC-LTE dissector (epan/dissectors/packet-mac-lte.c) in Wireshark 1.2.0 through 1.2.13 and 1.4.0 through 1.4.2 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large number of RARs.

The vulnerability is reported in versions 1.2.0 through 1.2.13 and 1.4.0 through 1.4.2.

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

References:

- * MISC:
<https://bugs.wireshark.org/bugzilla/attachment.cgi?id=5676>
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2011-01.html>
- * CONFIRM:
<http://www.wireshark.org/security/wnpa-sec-2011-02.html>
- * CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=5530
- * FEDORA: FEDORA-2011-0450
<http://lists.fedoraproject.org/pipermail/package-announce/2011-February/053650.html>
- * FEDORA: FEDORA-2011-0460
<http://lists.fedoraproject.org/pipermail/package-announce/2011-February/053669.html>
- * MANDRIVA: MDVSA-2011:007
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:007>
- * REDHAT: RHSA-2011:0369
<http://www.redhat.com/support/errata/RHSA-2011-0369.html>
- * BID: 45775
<http://www.securityfocus.com/bid/45775>

* OSVDB: 70403
<http://osvdb.org/70403>
* SECUNIA: 43175
<http://secunia.com/advisories/43175>
* VUPEN: ADV-2011-0079
<http://www.vupen.com/english/advisories/2011/0079>
* VUPEN: ADV-2011-0104
<http://www.vupen.com/english/advisories/2011/0104>
* VUPEN: ADV-2011-0270
<http://www.vupen.com/english/advisories/2011/0270>
* VUPEN: ADV-2011-0719
<http://www.vupen.com/english/advisories/2011/0719>
* XF: wireshark-maclte-bo(64624)
<http://xforce.iss.net/xforce/xfdb/64624>

CVE Reference:

CVE-2011-0444 (cve.mitre.org, nvd.nist.gov)

• 19346 Wireshark ENTTEC dissector overflow Vulnerability (Remote File Checking)

Buffer overflow in the sect_enttec_dmx_da function in epan/dissectors/packet-enttec.c in Wireshark 1.4.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted ENTTEC DMX packet with Run Length Encoding (RLE) compression.

The vulnerability is reported in versions 1.2.0 through 1.2.13 and 1.4.0 through 1.4.2.

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

References:

* MLIST: [oss-security] 20101231 CVE Request: Wireshark
<http://openwall.com/lists/oss-security/2010/12/31/7>
* MLIST: [oss-security] 20110103 Re: CVE Request: Wireshark
<http://openwall.com/lists/oss-security/2011/01/03/8>
* CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=5539
* DEBIAN: DSA-2144
<http://www.debian.org/security/2011/dsa-2144>
* FEDORA: FEDORA-2011-0128
<http://lists.fedoraproject.org/pipermail/package-announce/2011-January/053042.html>
* FEDORA: FEDORA-2011-0167
<http://lists.fedoraproject.org/pipermail/package-announce/2011-January/053061.html>
* MANDRIVA: MDVSA-2011:002
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:002>
* REDHAT: RHSA-2011:0013
<http://www.redhat.com/support/errata/RHSA-2011-0013.html>
* BID: 45634
<http://www.securityfocus.com/bid/45634>
* OSVDB: 70244
<http://osvdb.org/70244>
* SECTRACK: 1024930
<http://www.securitytracker.com/id?1024930>
* SECUNIA: 42767
<http://secunia.com/advisories/42767>
* SECUNIA: 42853
<http://secunia.com/advisories/42853>
* SECUNIA: 42914
<http://secunia.com/advisories/42914>
* SECUNIA: 42910
<http://secunia.com/advisories/42910>
* VUPEN: ADV-2011-0079
<http://www.vupen.com/english/advisories/2011/0079>
* VUPEN: ADV-2011-0008
<http://www.vupen.com/english/advisories/2011/0008>
* VUPEN: ADV-2011-0053
<http://www.vupen.com/english/advisories/2011/0053>
* VUPEN: ADV-2011-0069
<http://www.vupen.com/english/advisories/2011/0069>
* VUPEN: ADV-2011-0099
<http://www.vupen.com/english/advisories/2011/0099>

* VUPEN: ADV-2011-0110
<http://www.vupen.com/english/advisories/2011/0110>

CVE Reference:

CVE-2010-4538 (cve.mitre.org, nvd.nist.gov)

• 19347 Wireshark ASN.1 BER dissector crash Vulnerability (Remote File Checking)

The ASN.1 BER dissector in Wireshark 1.4.0 through 1.4.2 allows remote attackers to cause a denial of service (assertion failure) via crafted packets, as demonstrated by fuzz-2010-12-30-28473.pcap.

The vulnerability is reported in versions 1.4.0 through 1.4.2.

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

References:

- * CONFIRM:
<http://www.wireshark.org/security/wmpa-sec-2011-02.html>
- * CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=5537
- * FEDORA: FEDORA-2011-0450
<http://lists.fedoraproject.org/pipermail/package-announce/2011-February/053650.html>
- * FEDORA: FEDORA-2011-0460
<http://lists.fedoraproject.org/pipermail/package-announce/2011-February/053669.html>
- * BID: 45775
<http://www.securityfocus.com/bid/45775>
- * OSVDB: 70402
<http://osvdb.org/70402>
- * SECUNIA: 43175
<http://secunia.com/advisories/43175>
- * VUPEN: ADV-2011-0079
<http://www.vupen.com/english/advisories/2011/0079>
- * VUPEN: ADV-2011-0270
<http://www.vupen.com/english/advisories/2011/0270>
- * XF: wireshark-asn1ber-disssector-dos(64625)
<http://xforce.iss.net/xforce/xfdb/64625>

CVE Reference:

CVE-2011-0445 (cve.mitre.org, nvd.nist.gov)

• 19348 Wireshark freeing uninitialized pointer Vulnerability (Remote File Checking)

Wireshark 1.2.0 through 1.2.14, 1.4.0 through 1.4.3, and 1.5.0 frees an uninitialized pointer during processing of a .pcap file in the pcap-ng format, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a malformed file.

The vulnerability is reported in versions 1.2.0 through 1.2.14, 1.4.0 through 1.4.3, and 1.5.0.

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

References:

- * MLIST: [oss-security] 20110204 Wireshark: Freeing uninitialized pointer
<http://openwall.com/lists/oss-security/2011/02/04/1>
- * MISC:
<https://srcm.symantec.com/EditVulnerabilityFixes.aspx?docId=549474>
- * CONFIRM:
https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=5652
- * 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/wmpa-sec-2011-03.html>
- * CONFIRM:
<http://www.wireshark.org/security/wmpa-sec-2011-04.html>
- * CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=676232
- * 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>
* BID: 46167
<http://www.securityfocus.com/bid/46167>
* 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>
* XF: wireshark-pcap-code-execution(65182)
<http://xforce.iss.net/xforce/xfdb/65182>

CVE Reference:

CVE-2011-0538 (cve.mitre.org, nvd.nist.gov)

● 19349 Wireshark Nokia DCT3 overflow Vulnerability (Remote File Checking)

Heap-based buffer overflow in wiretap/dct3trace.c in Wireshark 1.2.0 through 1.2.14 and 1.4.0 through 1.4.3 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a long record in a Nokia DCT3 trace file.

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

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

References:

* MLIST: [oss-security] 20110216 wireshark dct3trace buffer overflow
<http://openwall.com/lists/oss-security/2011/02/16/13>
* CONFIRM:
<http://anonsvn.wireshark.org/viewvc?view=rev&revision=35953>
* 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://bugzilla.redhat.com/show_bug.cgi?id=678198
* 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-2011:0369
<http://www.redhat.com/support/errata/RHSA-2011-0369.html>
* BID: 46416
<http://www.securityfocus.com/bid/46416>
* SECTRACK: 1025148
<http://www.securitytracker.com/id?1025148>
* 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>

* XF: wireshark-visualc-bo(65460)
<http://xforce.iss.net/xforce/xfdb/65460>
* XF: wireshark-nokiadct3-bo(65780)
<http://xforce.iss.net/xforce/xfdb/65780>

CVE Reference:

CVE-2011-0713 (cve.mitre.org, nvd.nist.gov)

• 19350 Wireshark pcap-ng file with large packet-length field Vulnerability (Remote File Checking)

wiretap/pcapng.c in Wireshark 1.2.0 through 1.2.14 and 1.4.0 through 1.4.3 allows remote attackers to cause a denial of service (application crash) via a pcap-ng file that contains a large packet-length field.

The vulnerability is reported in versions 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=35855>
* 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=5661
* 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>
* XF: wireshark-pcapng-dos(65779)
<http://xforce.iss.net/xforce/xfdb/65779>

CVE Reference:

CVE-2011-1139 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-0546 Symantec CVSS 2.0 Score = 6.5

Symantec Backup Exec 11.0, 12.0, 12.5, 13.0, and 13.0 R2 does not validate identity information sent between the media server and the remote agent, which allows man-in-the-middle attackers to execute NDMP commands via unspecified vectors.

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

References:

CONFIRM:

http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory

BID: <http://www.securityfocus.com/bid/47824>

SECUNIA: <http://secunia.com/advisories/44698>

CVE Reference: [CVE-2011-0546](#)

• **CVE-2011-1512 IBM CVSS 2.0 Score = 9.3**

Heap-based buffer overflow in xlsr.dll in Autonomy KeyView, as used in IBM Lotus Notes before 8.5.2 FP3, allows remote attackers to execute arbitrary code via a malformed BIFF record in a .xls Excel spreadsheet attachment, aka SPR PRAD8E3HKR.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/67619>

BID: <http://www.securityfocus.com/bid/47962>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/518120/100/0/threaded>

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg21500034>

MISC: <http://www.coresecurity.com/content/LotusNotes-XLS-viewer-heap-overflow>

SECUNIA: <http://secunia.com/advisories/44624>

CVE Reference: [CVE-2011-1512](#)

• **CVE-2011-1218 IBM CVSS 2.0 Score = 9.3**

Buffer overflow in kvarcve.dll in Autonomy KeyView, as used in IBM Lotus Notes before 8.5.2 FP3, allows remote attackers to execute arbitrary code via a crafted .zip attachment, aka SPR PRAD8E3NSP. NOTE: some of these details are obtained from third party information.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/67625>

BID: <http://www.securityfocus.com/bid/47962>

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg21500034>

SECUNIA: <http://secunia.com/advisories/44624>

CVE Reference: [CVE-2011-1218](#)

• **CVE-2011-1217 IBM CVSS 2.0 Score = 9.3**

Buffer overflow in kppzrdr.dll in Autonomy KeyView, as used in IBM Lotus Notes before 8.5.2 FP3, allows remote attackers to execute arbitrary code via a crafted .prz attachment. NOTE: some of these details are obtained from third party information.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/67624>

BID: <http://www.securityfocus.com/bid/47962>

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg21500034>

SECUNIA: <http://secunia.com/advisories/44624>

CVE Reference: [CVE-2011-1217](#)

• **CVE-2011-1215 IBM CVSS 2.0 Score = 9.3**

Stack-based buffer overflow in mw8sr.dll in Autonomy KeyView, as used in IBM Lotus Notes before 8.5.2 FP3, allows remote attackers to execute arbitrary code via a crafted link in a Microsoft Office document attachment, aka SPR PRAD8823ND.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/67622>

BID: <http://www.securityfocus.com/bid/47962>

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg21500034>

SECUNIA: <http://secunia.com/advisories/44624>

IDEFENSE: <http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=906>

CVE Reference: [CVE-2011-1215](#)

• **CVE-2011-1216 IBM CVSS 2.0 Score = 9.3**

Stack-based buffer overflow in assr.dll in Autonomy KeyView, as used in IBM Lotus Notes before 8.5.2 FP3, allows remote attackers to execute arbitrary code via crafted tag data in an Applix spreadsheet attachment, aka SPR PRAD8823A7.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/67623>

BID: <http://www.securityfocus.com/bid/47962>

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg21500034>

SECUNIA: <http://secunia.com/advisories/44624>

IDEFENSE: <http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=907>

CVE Reference: [CVE-2011-1216](#)

• **CVE-2011-1214 IBM CVSS 2.0 Score = 9.3**

Stack-based buffer overflow in rtfsr.dll in Autonomy KeyView, as used in IBM Lotus Notes before 8.5.2 FP3, allows remote attackers to execute arbitrary code via a crafted link in a .rtf attachment, aka SPR PRAD8823JQ.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/67621>

BID: <http://www.securityfocus.com/bid/47962>

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg21500034>

SECUNIA: <http://secunia.com/advisories/44624>

IDEFENSE: <http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=905>

CVE Reference: [CVE-2011-1214](#)

• **CVE-2011-1213 IBM CVSS 2.0 Score = 9.3**

Integer underflow in lzhsr.dll in Autonomy KeyView, as used in IBM Lotus Notes before 8.5.2 FP3, allows remote attackers to execute arbitrary code via a crafted header in a .lzh attachment that triggers a stack-based buffer overflow, aka SPR PRAD88MJ2W.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/67620>

BID: <http://www.securityfocus.com/bid/47962>

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg21500034>

SECUNIA: <http://secunia.com/advisories/44624>

IDEFENSE: <http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=904>

CVE Reference: [CVE-2011-1213](#)

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