

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://www.netvigilance.com/productdownloads?productname=apachechunkedvulnerabilityscanner>

This Week in Review

java exploits surpass PDF reader exploits. And electronic thefts surpass physical ones. Problematic usage of Facebook brought to court. Botnet used to influence stock.

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

• Microsoft warns of "unprecedented" Java exploitation

The number of attacks on vulnerable Java code spiked during the third quarter of the year and have reached "unprecedented" levels, a Microsoft malware expert said on Monday.

The increase was largely attributable to attacks on three Java vulnerabilities, all of which have patches available, Holly Stewart, senior program manager at Microsoft, wrote in a blog post Monday.

But despite the fixes being available from Oracle, the number of attacks against the flaws increased from hundreds of thousands per quarter to more than six million during the third quarter of 2010, Stewart said. Even by the start of the year - months before the spike - Java exploits already well outnumbered Adobe-related exploits. SC Magazine

Full Story :

http://www.scmagazineus.com/microsoft-warns-of-unprecedented-java-exploitation/article/181205/?utm_source=feed

• Study: Electronic theft surpasses physical theft

For the first time ever, more companies are suffering from electronic theft than from physical theft, according to the results of a poll released yesterday by risk consultancy Kroll.

The firm's fourth "Annual Global Fraud Report" (PDF) found that the amount of money lost by businesses to all kinds of fraud rose over the past 12 months to \$1.7 million per billion dollars of sales from \$1.4 million, a gain of more than 20 percent.

And with that overall increase came a notable shift, with electronic theft just edging out physical theft. The theft of information or electronic assets was reported by 27.3 percent of companies over the past 12 months, up from 18 percent in 2009. The theft of physical assets inched down to 27.2 percent from 28 percent last year. Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20019999-83.html?part=rss&subj=news&tag=2547-1_3-0-20

• Facebook files three antispam lawsuits

Facebook announced today that it has filed suit against two individuals and a company that it says are responsible for propagating deceptive spam offers across the massive social network, including some that encouraged members to spam their friends in turn.

"This week, in a U.S. federal court in San Jose, California, we filed three lawsuits alleging violations of our terms and applicable law by defendants attempting to trick people on Facebook into signing up for mobile subscriptions and sending spam to their friends," a blog entry posted by Facebook's security team explained. "In three separate complaints, we allege that Steven Richter, Jason Swan, and Max Bounty, Inc. used Facebook to offer enticing, but non-existent products and services." Cnet Security

Full Story :

http://news.cnet.com/8301-13577_3-20020217-36.html?part=rss&subj=news&tag=2547-1_3-0-20

• Man pleads guilty to using hack, pump-and-dump botnet

IDG News Service - A Chandler, Ariz., man has pleaded guilty to charges related to his role in a pump-and-dump scam that inflated penny stock prices via spam and hacked computers.

James Bragg, 41, faces five years in prison and a \$250,000 fine for orchestrating the hacking and spamming portions of the scheme, which ran between November 2007 and February 2009, according to prosecutors. He pleaded guilty Wednesday in U.S. District Court for the District of New Jersey.

Bragg used a Russian botnet operator, named only as B.T. in court documents, to send the spam and to access hacked brokerage accounts and buy the penny stocks without the victim's knowledge. Computerworld

Full Story :

http://www.computerworld.com/s/article/9192120/Man_pleads_guilty_to_using_hack_pump_and_dump_botnet?sour

New Vulnerabilities Tested in SecureScout

• 18962 Uninitialized Memory Corruption Vulnerability (CVE-2010-3331) (MS10-071/2360131) (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. An attacker could exploit the vulnerability by convincing a user to view a specially crafted Word document. When a user closes the Word document, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could 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:

* MS: MS10-071

<http://www.microsoft.com/technet/security/bulletin/ms10-071.msp>

* BID: 43707

<http://www.securityfocus.com/bid/43707>

* VUPEN: VUPEN/ADV-2010-2618

<http://www.vupen.com/english/advisories/2010/2618>

* SECTRACK: 1024546

<http://securitytracker.com/alerts/2010/Oct/1024546.html>

CVE Reference:

CVE-2010-3331 (cve.mitre.org, nvd.nist.gov)

• 18964 Word Uninitialized Pointer Vulnerability (MS10-079/2293194) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Word handles an uninitialized pointer when parsing a specially crafted Word file. An attacker who successfully exploited this vulnerability could 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* MS: MS10-079

<http://www.microsoft.com/technet/security/Bulletin/MS10-079.msp>

* VUPEN: VUPEN/ADV-2010-2626

<http://www.vupen.com/english/advisories/2010/2626>

* SECTRACK: 1024551

<http://securitytracker.com/alerts/2010/Oct/1024551.html>

* BID: 43754

<http://www.securityfocus.com/bid/43754>

CVE Reference:

CVE-2010-2747 (cve.mitre.org, nvd.nist.gov)

• 18965 Word Boundary Check Vulnerability (MS10-079/2293194) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Word handles an improper boundary check when parsing a specially crafted Word file. An attacker who successfully exploited this vulnerability could 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* MS: MS10-079

<http://www.microsoft.com/technet/security/Bulletin/MS10-079.msp>

* VUPEN: VUPEN/ADV-2010-2626

<http://www.vupen.com/english/advisories/2010/2626>

* SECTRACK: 1024551

<http://securitytracker.com/alerts/2010/Oct/1024551.html>

* BID: 43765

<http://www.securityfocus.com/bid/43765>

CVE Reference:

CVE-2010-2748 (cve.mitre.org, nvd.nist.gov)

• 18966 Word Index Vulnerability (MS10-079/2293194) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Word handles index values inside a specially crafted Word file. An attacker who successfully exploited this vulnerability could 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* MS: MS10-079

<http://www.microsoft.com/technet/security/Bulletin/MS10-079.msp>

* VUPEN: VUPEN/ADV-2010-2626

<http://www.vupen.com/english/advisories/2010/2626>

* SECTRACK: 1024551

<http://securitytracker.com/alerts/2010/Oct/1024551.html>

* BID: 43766

<http://www.securityfocus.com/bid/43766>

CVE Reference:

CVE-2010-2750 (cve.mitre.org, nvd.nist.gov)

• 18967 Word Stack Overflow Vulnerability (MS10-079/2293194) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Word handles stack validation when parsing a specially crafted Word file. An attacker who successfully exploited this vulnerability could 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

- * MS: MS10-079
<http://www.microsoft.com/technet/security/Bulletin/MS10-079.msp>
- * VUPEN: VUPEN/ADV-2010-2626
<http://www.vupen.com/english/advisories/2010/2626>
- * SECTRACK: 1024551
<http://securitytracker.com/alerts/2010/Oct/1024551.html>
- * BID: 43760
<http://www.securityfocus.com/bid/43760>

CVE Reference:

CVE-2010-3214 (cve.mitre.org, nvd.nist.gov)
CVE-2010-3214 (cve.mitre.org, nvd.nist.gov)

• 18968 Word Return Value Vulnerability (MS10-079/2293194) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Word handles return values when parsing a specially crafted Word file. An attacker who successfully exploited this vulnerability could 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

- * MS: MS10-079
<http://www.microsoft.com/technet/security/Bulletin/MS10-079.msp>
- * VUPEN: VUPEN/ADV-2010-2626
<http://www.vupen.com/english/advisories/2010/2626>
- * SECTRACK: 1024551
<http://securitytracker.com/alerts/2010/Oct/1024551.html>
- * BID: 43767
<http://www.securityfocus.com/bid/43767>

CVE Reference:

CVE-2010-3215 (cve.mitre.org, nvd.nist.gov)

• 18969 Word Bookmarks Vulnerability (MS10-079/2293194) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Word handles bookmarks when parsing a specially crafted Word file. An attacker who successfully exploited this vulnerability could 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

- * MS: MS10-079
<http://www.microsoft.com/technet/security/Bulletin/MS10-079.msp>
- * VUPEN: VUPEN/ADV-2010-2626
<http://www.vupen.com/english/advisories/2010/2626>
- * SECTRACK: 1024551
<http://securitytracker.com/alerts/2010/Oct/1024551.html>
- * BID: 43769
<http://www.securityfocus.com/bid/43769>

CVE Reference:

CVE-2010-3216 (cve.mitre.org, nvd.nist.gov)

• 18970 Word Pointer Vulnerability (MS10-079/2293194) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Word handles pointers when parsing a specially crafted Word file. An attacker who successfully exploited this vulnerability could 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* MS: MS10-079

<http://www.microsoft.com/technet/security/Bulletin/MS10-079.mspx>

* VUPEN: VUPEN/ADV-2010-2626

<http://www.vupen.com/english/advisories/2010/2626>

* SECTRACK: 1024551

<http://securitytracker.com/alerts/2010/Oct/1024551.html>

* BID: 43770

<http://www.securityfocus.com/bid/43770>

CVE Reference:

CVE-2010-3217 (cve.mitre.org, nvd.nist.gov)

• 18971 Word Heap Overflow Vulnerability (MS10-079/2293194) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Word handles malformed records inside a specially crafted Word file. An attacker who successfully exploited this vulnerability could 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* MS: MS10-079

<http://www.microsoft.com/technet/security/Bulletin/MS10-079.mspx>

* VUPEN: VUPEN/ADV-2010-2626

<http://www.vupen.com/english/advisories/2010/2626>

* SECTRACK: 1024551

<http://securitytracker.com/alerts/2010/Oct/1024551.html>

* BID: 43771

<http://www.securityfocus.com/bid/43771>

CVE Reference:

CVE-2010-3218 (cve.mitre.org, nvd.nist.gov)

• 18972 Word Index Parsing Vulnerability (MS10-079/2293194) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Word handles indexes when parsing a specially crafted Word file. An attacker who successfully exploited this vulnerability could 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* MS: MS10-079

<http://www.microsoft.com/technet/security/Bulletin/MS10-079.mspx>

* VUPEN: VUPEN/ADV-2010-2626

<http://www.vupen.com/english/advisories/2010/2626>

* SECTRACK: 1024551

<http://securitytracker.com/alerts/2010/Oct/1024551.html>

* BID: 43782

<http://www.securityfocus.com/bid/43782>

CVE Reference:

CVE-2010-3219 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-0219 Apache CVSS 2.0 Score = 10.0

Apache Axis2, as used in dswsbobje.war in SAP BusinessObjects Enterprise XI 3.2 and other products, has a default password of axis2 for the admin account, which makes it easier for remote attackers to execute arbitrary code by uploading a crafted web service.

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

References:

CERT-VN: <http://www.kb.cert.org/vuls/id/989719>

MISC: <https://service.sap.com/sap/support/notes/1432881>

XF: <http://xforce.iss.net/xforce/xfdb/62523>

VUPEN: <http://www.vupen.com/english/advisories/2010/2673>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/514284/100/0/threaded>

MISC: <http://www.rapid7.com/security-center/advisories/R7-0037.jsp>

MISC: http://spl0it.org/files/talks/source_barcelona10/Hacking%20SAP%20BusinessObjects.pdf

SECUNIA: <http://secunia.com/advisories/41799>

CVE Reference: [CVE-2010-0219](#)

• CVE-2009-5005 Apache CVSS 2.0 Score = 5.0

The Cluster::deliveredEvent function in cluster/Cluster.cpp in Apache Qpid, as used in Red Hat Enterprise MRG before 1.3 and other products, allows remote attackers to cause a denial of service (daemon crash and cluster outage) via invalid AMQP data.

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

References:

REDHAT: <https://rhn.redhat.com/errata/RHSA-2010-0774.html>

REDHAT: <https://rhn.redhat.com/errata/RHSA-2010-0773.html>

CONFIRM: <http://svn.apache.org/viewvc?revision=785788&view=revision>

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=642373

VUPEN: <http://www.vupen.com/english/advisories/2010/2684>

SECUNIA: <http://secunia.com/advisories/41812>

SECUNIA: <http://secunia.com/advisories/41710>

CVE Reference: [CVE-2009-5005](#)

• CVE-2010-2057 Apache CVSS 2.0 Score = 5.0

shared/util/StateUtils.java in Apache MyFaces 1.1.x before 1.1.8, 1.2.x before 1.2.9, and 2.0.x before 2.0.1 uses an encrypted View State without a Message Authentication Code (MAC), which makes it easier for remote attackers to perform successful modifications of the View State via a padding oracle attack.

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

References:

CONFIRM:

<http://svn.apache.org/viewvc/myfaces/shared/trunk/core/src/main/java/org/apache/myfaces/shared/util/StateUtils.java?r1=>

CONFIRM: <https://issues.apache.org/jira/browse/MYFACES-2749>

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=623799

CVE Reference: [CVE-2010-2057](#)

• **CVE-2009-5006 Apache CVSS 2.0 Score = 4.0**

The SessionAdapter::ExchangeHandlerImpl::checkAlternate function in broker/SessionAdapter.cpp in the C++ Broker component in Apache Qpid before 0.6, as used in Red Hat Enterprise MRG before 1.3 and other products, allows remote authenticated users to cause a denial of service (NULL pointer dereference, daemon crash, and cluster outage) by attempting to modify the alternate of an exchange. Per: <http://cwe.mitre.org/data/definitions/476.html> 'CWE-476: NULL Pointer Dereference'

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

References:

REDHAT: <https://rhn.redhat.com/errata/RHSA-2010-0774.html>

REDHAT: <https://rhn.redhat.com/errata/RHSA-2010-0773.html>

CONFIRM: <https://issues.apache.org/jira/browse/QPID-2080>

CONFIRM: <http://svn.apache.org/viewvc?revision=811188&view=revision>

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=642377

VUPEN: <http://www.vupen.com/english/advisories/2010/2684>

SECUNIA: <http://secunia.com/advisories/41812>

SECUNIA: <http://secunia.com/advisories/41710>

CVE Reference: [CVE-2009-5006](#)

• **CVE-2010-4007 Oracle CVSS 2.0 Score = 5.0**

Oracle Mojarra uses an encrypted View State without a Message Authentication Code (MAC), which makes it easier for remote attackers to perform successful modifications of the View State via a padding oracle attack, a related issue to CVE-2010-2057.

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

References:

MISC: <https://issues.apache.org/jira/browse/MYFACES-2749>

MISC: https://bugzilla.redhat.com/show_bug.cgi?id=623799

CVE Reference: [CVE-2010-4007](#)

• **CVE-2010-3287 HP CVSS 2.0 Score = 8.3**

Unspecified vulnerability on HP ProCurve Access Points, Access Controllers, and Mobility Controllers with software 5.1.x through 5.1.9, 5.2.x through 5.2.7, 5.3.x through 5.3.5, and 5.4.x through 5.4.0 allows remote attackers to execute arbitrary code via unknown vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=128708618023203&w=2>

HP: <http://marc.info/?l=bugtraq&m=128708618023203&w=2>

CVE Reference: [CVE-2010-3287](#)

• **CVE-2010-3286 HP CVSS 2.0 Score = 5.0**

Unspecified vulnerability in HP Systems Insight Manager (SIM) 6.0 and 6.1 allows remote attackers to read arbitrary files via unknown vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=128706731926760&w=2>

HP: <http://marc.info/?l=bugtraq&m=128706731926760&w=2>

CVE Reference: [CVE-2010-3286](#)

• CVE-2010-3748 RealNetworks CVSS 2.0 Score = 10.0

Stack-based buffer overflow in the RichFX component in RealNetworks RealPlayer 11.0 through 11.1, RealPlayer SP 1.0 through 1.1.4, and RealPlayer Enterprise 2.1.2 allows remote attackers to have an unspecified impact via unknown vectors.

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

References:

BID: <http://www.securityfocus.com/bid/44144>

CONFIRM: http://service.real.com/realplayer/security/10152010_player/en/

CVE Reference: [CVE-2010-3748](#)

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