

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

Large botnet taken down by Holland and Armenia. First-ever Russian spam case. Beware of Boonana. American support for presidential internet shut-down.

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

• Dutch team up with Armenia for Bredolab botnet take down

IDG News Service - Armenian authorities arrested a 27-year-old man on Tuesday on suspicion of running a large botnet that was dismantled after a unique take-down operation by Dutch law enforcement and computer security experts on Monday.

Dutch authorities said they seized dozens of servers used to control the Bredolab botnet, estimated to have infected millions of computers worldwide.

Bredolab is a type of malicious software program that can steal login and password details, log keystrokes, and steal any data from an infected computer. The Dutch High Tech Crime Team, which is part of the National Crime Squad, began investigating the botnet over the summer, according to a press release issued on Monday. Computerworld

Full Story :

http://www.computerworld.com/s/article/9193080/Dutch_team_up_with_Armenia_for_Bredolab_botnet_take_down?s

• **Russia files criminal case against major spammer**

IDG News Service - Russia has reportedly launched its first-ever criminal case related to spam against a man accused of running one of the world's most prolific pharmaceutical spam operations, according to local news reports.

The investigation focuses on Igor Gusev, who is general director of the company Despmedia, which is affiliated with Glavmed.com, a site that appears to be an affiliate program related to driving traffic to Web sites selling drugs over the Internet, according to RIA Novosti, citing the Kommersant newspaper.

Despmedia has generated \$120 million in revenue since 2007, with Gusev netting \$2 million, Kommersant reported.
Computerworld

Full Story :

http://www.computerworld.com/s/article/9193358/Russia_files_criminal_case_against_major_spammer?source=rss

• **Critical security risk posed by new 'Boonana' Trojan horse for OS X**

A new Trojan horse malware that affects Mac OS X has been uncovered by Macintosh Security site SecureMac. The Trojan is called "trojan.osx.boonana.a" and is being disguised as a video and distributed through social-networking sites like Facebook.

The Trojan horse appears as a link on people's Facebook pages that may have the text "Is this you in this video?" in the link. When the link is clicked, the Trojan will run a Java applet that will download other files to the computer and run an installer automatically.

The Trojan will run in the background and appears to report system information to servers on the Internet, which can be a big breach of personal information. The Trojan also will attempt to spread itself by sending messages from the user account to other people through spam e-mail messages. Cnet Security

Full Story :

http://reviews.cnet.com/8301-13727_7-20020892-263.html?part=rss&subj=news&tag=2547-1_3-0-20

• **Study finds support for presidential Net 'kill switch'**

If the U.S. were hit by a severe cyberattack, would you want the president to be able to control or even shut down portions of the Internet?

A majority 61 percent of Americans polled by Unisys for a new security study believes the president should have the power to control or effectively "kill" portions of the Internet if key U.S. systems (military, financial, electrical) were hit by a malicious cyberattack from a foreign government.

These findings from the latest biannual Unisys Security Index suggest that the public may support a pending cybersecurity bill that would give the president greater authority over the Internet in the event of an emergency. Formally known as the Protecting Cyberspace as a National Asset Act, or PCNAA, the bill (PDF) would grant the government the power to force Internet providers, search engines, software firms, and other private companies to comply with emergency measures established by the Department of Homeland Security. Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20020901-83.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• **18973 Word Parsing Vulnerability (CVE-2010-3220) (MS10-079/2293194) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Word parses 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>

* SECTRAK: 1024551

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

* BID: 43783

<http://www.securityfocus.com/bid/43783>

CVE Reference:

CVE-2010-3220 (cve.mitre.org, nvd.nist.gov)

• 18974 Word Parsing Vulnerability (CVE-2010-3221) (MS10-079/2293194) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Word parses 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: 43784

<http://www.securityfocus.com/bid/43784>

CVE Reference:

CVE-2010-3221 (cve.mitre.org, nvd.nist.gov)

• 18975 Excel Record Parsing Integer Overflow Vulnerability (MS10-080/2293211) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. 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: MS10-080

<http://www.microsoft.com/technet/security/Bulletin/MS10-080.mspx>

* BID: 43643

<http://www.securityfocus.com/bid/43643>

* VUPEN: VUPEN/ADV-2010-2627

<http://www.vupen.com/english/advisories/2010/2627>

* SECTRACK: 1024552

<http://securitytracker.com/alerts/2010/Oct/1024552.html>

CVE Reference:

CVE-2010-3230 (cve.mitre.org, nvd.nist.gov)

• 18976 Excel Record Parsing Memory Corruption Vulnerability (MS10-080/2293211) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. 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: MS10-080

<http://www.microsoft.com/technet/security/Bulletin/MS10-080.mspx>

* BID: 43647

<http://www.securityfocus.com/bid/43647>

* VUPEN: VUPEN/ADV-2010-2627

<http://www.vupen.com/english/advisories/2010/2627>

* SECTRACK: 1024552

<http://securitytracker.com/alerts/2010/Oct/1024552.html>

CVE Reference:

CVE-2010-3231 (cve.mitre.org, nvd.nist.gov)

• 18977 Excel File Format Parsing Vulnerability (MS10-080/2293211) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. 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: MS10-080
<http://www.microsoft.com/technet/security/Bulletin/MS10-080.msp>
- * BID: 43646
<http://www.securityfocus.com/bid/43646>
- * VUPEN: VUPEN/ADV-2010-2627
<http://www.vupen.com/english/advisories/2010/2627>
- * SECTRACK: 1024552
<http://securitytracker.com/alerts/2010/Oct/1024552.html>

CVE Reference:

CVE-2010-3232 (cve.mitre.org, nvd.nist.gov)

• 18978 Lotus 1-2-3 Workbook Parsing Vulnerability (MS10-080/2293211) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Lotus 1-2-3 workbook files (.wk3). 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: MS10-080
<http://www.microsoft.com/technet/security/Bulletin/MS10-080.msp>
- * BID: 43644
<http://www.securityfocus.com/bid/43644>
- * VUPEN: VUPEN/ADV-2010-2627
<http://www.vupen.com/english/advisories/2010/2627>
- * SECTRACK: 1024552
<http://securitytracker.com/alerts/2010/Oct/1024552.html>

CVE Reference:

CVE-2010-3233 (cve.mitre.org, nvd.nist.gov)

• 18979 Formula Substream Memory Corruption Vulnerability (MS10-080/2293211) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. 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: MS10-080
<http://www.microsoft.com/technet/security/Bulletin/MS10-080.msp>
- * BID: 43649
<http://www.securityfocus.com/bid/43649>
- * VUPEN: VUPEN/ADV-2010-2627
<http://www.vupen.com/english/advisories/2010/2627>
- * SECTRACK: 1024552
<http://securitytracker.com/alerts/2010/Oct/1024552.html>

CVE Reference:

CVE-2010-3234 (cve.mitre.org, nvd.nist.gov)

• 18980 Formula Biff Record Vulnerability (MS10-080/2293211) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. 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: MS10-080
<http://www.microsoft.com/technet/security/Bulletin/MS10-080.msp>
- * BID: 43650
<http://www.securityfocus.com/bid/43650>
- * VUPEN: VUPEN/ADV-2010-2627
<http://www.vupen.com/english/advisories/2010/2627>
- * SECTRACK: 1024552
<http://securitytracker.com/alerts/2010/Oct/1024552.html>

CVE Reference:

CVE-2010-3235 (cve.mitre.org, nvd.nist.gov)

• 18981 Out Of Bounds Array Vulnerability (MS10-080/2293211) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. 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: MS10-080
<http://www.microsoft.com/technet/security/Bulletin/MS10-080.msp>
- * BID: 43651
<http://www.securityfocus.com/bid/43651>
- * VUPEN: VUPEN/ADV-2010-2627
<http://www.vupen.com/english/advisories/2010/2627>
- * SECTRACK: 1024552
<http://securitytracker.com/alerts/2010/Oct/1024552.html>

CVE Reference:

CVE-2010-3236 (cve.mitre.org, nvd.nist.gov)

• 18982 Merge Cell Record Pointer Vulnerability (MS10-080/2293211) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Excel handles specially crafted Excel files. 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: MS10-080
<http://www.microsoft.com/technet/security/Bulletin/MS10-080.msp>
- * BID: 43652
<http://www.securityfocus.com/bid/43652>
- * VUPEN: VUPEN/ADV-2010-2627
<http://www.vupen.com/english/advisories/2010/2627>
- * SECTRACK: 1024552
<http://securitytracker.com/alerts/2010/Oct/1024552.html>

CVE Reference:

CVE-2010-3237 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-3227 Microsoft CVSS 2.0 Score = 9.3

Stack-based buffer overflow in the UpdateFrameTitleForDocument method in the CFrameWnd class in mfc42.dll in the Microsoft Foundation Class (MFC) Library in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2,

Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows context-dependent attackers to execute arbitrary code via a long window title that this library attempts to create at the request of an application, as demonstrated by the Trident PowerZip 7.2 Build 4010 application, aka "Windows MFC Document Title Updating Buffer Overflow Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-074.msp>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/13921/>

MISC: <http://www.eeye.com/Resources/Security-Center/Research/Zero-Day-Tracker/2010/20100705-%281%29>

CVE Reference: [CVE-2010-3227](#)

• **CVE-2010-3288 HP CVSS 2.0 Score = 6.8**

Cross-site request forgery (CSRF) vulnerability in HP Systems Insight Manager (SIM) before 6.2 allows remote attackers to hijack the authentication of unspecified victims via unknown vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=128768031706686&w=2>

HP: <http://marc.info/?l=bugtraq&m=128768031706686&w=2>

CVE Reference: [CVE-2010-3288](#)

• **CVE-2010-3290 HP CVSS 2.0 Score = 6.5**

Unspecified vulnerability in HP Systems Insight Manager (SIM) before 6.2 allows remote authenticated users to gain privileges via unknown vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=128768031706686&w=2>

HP: <http://marc.info/?l=bugtraq&m=128768031706686&w=2>

CVE Reference: [CVE-2010-3290](#)

• **CVE-2010-3986 HP CVSS 2.0 Score = 5.0**

Unspecified vulnerability in HP Virtual Connect Enterprise Manager (VCEM) 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=128776031714107&w=2>

HP: <http://marc.info/?l=bugtraq&m=128776031714107&w=2>

CVE Reference: [CVE-2010-3986](#)

• **CVE-2010-3289 HP CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in HP Systems Insight Manager (SIM) before 6.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=128768031706686&w=2>

HP: <http://marc.info/?l=bugtraq&m=128768031706686&w=2>

CVE Reference: [CVE-2010-3289](#)

• **CVE-2010-4070 IBM CVSS 2.0 Score = 10.0**

Integer overflow in librpc.dll in portmap.exe (aka the ISM Portmapper service) in ISM before 2.20.TC1.117 in IBM Informix Dynamic Server (IDS) 7.x before 7.31.xD11, 9.x before 9.40.xC10, 10.00 before 10.00.xC8, and 11.10 before 11.10.xC2 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via a crafted parameter size, aka idsdb00146931, idsdb00146930, idsdb00146929, and idsdb00138308.

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

References:

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-10-215/>

VUPEN: <http://www.vupen.com/english/advisories/2010/2733>

OSVDB: <http://www.osvdb.org/68706>

SECUNIA: <http://secunia.com/advisories/41915>

CVE Reference: [CVE-2010-4070](#)

• **CVE-2010-4053 IBM CVSS 2.0 Score = 9.0**

Stack-based buffer overflow in an unspecified logging function in oninit.exe in IBM Informix Dynamic Server (IDS) 11.10 before 11.10.xC2W2 and 11.50 before 11.50.xC1 allows remote authenticated users to execute arbitrary code via a crafted EXPLAIN directive, aka idsdb00154125 and idsdb00154243.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/62619>

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-10-216/>

VUPEN: <http://www.vupen.com/english/advisories/2010/2734>

OSVDB: <http://www.osvdb.org/68705>

SECUNIA: <http://secunia.com/advisories/41913>

CVE Reference: [CVE-2010-4053](#)

• **CVE-2010-4069 IBM CVSS 2.0 Score = 8.5**

Stack-based buffer overflow in IBM Informix Dynamic Server (IDS) 7.x through 7.31, 9.x through 9.40, 10.00 before 10.00.xC10, 11.10 before 11.10.xC3, and 11.50 before 11.50.xC3 allows remote authenticated users to execute arbitrary code via long DBINFO keyword arguments in a SQL statement, aka idsdb00165017, idsdb00165019, idsdb00165021, idsdb00165022, and idsdb00165023.

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

References:

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-10-217/>

VUPEN: <http://www.vupen.com/english/advisories/2010/2735>

OSVDB: <http://www.osvdb.org/68707>

SECUNIA: <http://secunia.com/advisories/41914>

CVE Reference: [CVE-2010-4069](#)

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