ScoutNews
The weekly Security update from the makers of SecureScout
October 17, 2008

2008 Issue #42

Table of Contents

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

PricewaterhouseCoopers releases new security study. A call for closer coordination agains cyber crime. A flood of unsecure mobile devices. US Homeland Security views threats of cyber crime significant.

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

- **Study: Global information security improves, but still imperfect**

Information is the new currency of business and this year progress has been made to secure it, but there is still work to be done, according to a worldwide study released Wednesday at a seminar in New York.

The sixth annual study titled, "The State of Information Security 2008," was conducted in part by PricewaterhouseCoopers.

"How do you know what to protect if you don't know what you have and where it is?" Mark Lobel, a principal in the Advisory practice of PricewaterhouseCoopers, asked the audience Wednesday at the "2008 Global State of Information Security" seminar, held at PwC's headquarters in midtown Manhattan.

SC Magazine

Full Story :
http://www.scmagazineus.com/Study-Global-information-security-improves-but-still-imperfect/article/119517/

- **Academics predict growing cybercrime sophistication**

Data -- even on platforms such as mobile phones -- will continue to be the primary motive for future cybercrime. That's one of the key findings in asurvey released Wednesday by the Georgia Tech Information Security Center (GTISC).

The GTISC said it expects threats to rise and evolve in the areas of malware, botnets, cyberwarfare, VoIP and movile devices. It also foresees the continued sophistication of the criminal underground economy, in which cybercrooks peddle malware-for-sale kits and other programs.

A number of experts from across the IT security spectrum - from government to industry to academia - called, in the report, for closer coordination among the security industry, internet service providers (ISPs), application developers and government regulators to safeguard users and hinder the spread of sophisticated cybersecurity threats.

SC Magazine

Full Story :
http://www.scmagazineus.com/Academics-predict-growing-cybercrime-sophistication/article/119552/

- **Up next: Cellular botnets, cybermilitias**

October 17, 2008 (Computerworld) The ability of malware writers to consistently stay ahead of those seeking to stop them has been a constant factor in the security industry over the past several years.

The report was released this week by the Georgia Tech Information Security Center (GTISC) and looks at the threats that security managers are likely to confront next year and how to deal with them.

Bugs and botnets in the mobile world: The features built into smart phones, such as Apple's iPhone, Research In Motion's BlackBerry, Google's Android and Windows-enabled mobile devices, are making them increasingly computer-like in their functionality. And therein lies a security problem.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117424&source=rss_topic1

- **FBI: Several nations eye U.S. cybertargets**

October 15, 2008 (IDG News Service) About two-dozen nations have developed cyberattack capabilities and have their eyes on targets inside U.S. businesses and government agencies, the top cybercrime law enforcement official in the U.S. said today.

Henry declined to name the countries, but during a press conference he called organized attacks on U.S. cybertargets a "significant threat." Over the past year, cyberattacks against U.S. targets have become increasingly sophisticated, said Henry, who was appointed to the top post in the cyber division in September.

Henry encouraged government agencies and U.S. businesses to worry less about where cyberthreats are coming from and more about how to protect their data and networks.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117258&source=rss_topic1

New Vulnerabilities Tested in SecureScout

- **18150 Active Directory Overflow Vulnerability (MS08-060/957280) (Remote File Checking)**

A remote code execution vulnerability exists in implementations of Active Directory on Microsoft Windows 2000 Server. The vulnerability is due to incorrect memory allocation when receiving specially crafted LDAP or LDAPS requests. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

* MS: MS08-060
http://www.microsoft.com/technet/security/Bulletin/MS08-060.mspx
* SECUNIA: Microsoft Windows Active Directory Buffer Overflow Vulnerability
http://secunia.com/advisories/32242/
* BID: Microsoft Windows Active Directory LDAP Request Handling Remote Code Execution Vulnerability

http://www.securityfocus.com/bid/31609
* SECTRACK: 1021042
http://www.securitytracker.com/alerts/2008/Oct/1021042.html
* FRSIRT: FrSIRT/ADV-2008-2811
http://www.frsirt.com/english/advisories/2008/2811

CVE Reference:

CVE-2008-4023 (cve.mitre.org, nvd.nist.gov)

• 18151 Window Location Property Cross-Domain Vulnerability (MS08-058/956390) (Remote File Checking)

A remote code execution or information disclosure vulnerability exists in Internet Explorer that could allow an attacker to gain access to a browser window in another domain or Internet Explorer zone. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow remote code execution or information disclosure, depending on the operating system, if a user viewed the Web page.

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

References:

* MS: MS08-058
http://www.microsoft.com/technet/security/Bulletin/MS08-058.mspx
* SECUNIA: Internet Explorer 6 Window "location" Handling Vulnerability
http://secunia.com/advisories/30857/
* BID: Microsoft Internet Explorer 'location' & 'location.href' Cross Domain Security Bypass Vulnerability
http://www.securityfocus.com/bid/29960
* FRSIRT: FrSIRT/ADV-2008-2809
http://www.frsirt.com/english/advisories/2008/2809
* MISC:
http://blogs.zdnet.com/security/?p=1348
* MISC:
http://www.ph4nt0m.org-a.googlepages.com/PSTZine_0x02_0x04.txt
* CERT-VN: VU#923508
http://www.kb.cert.org/vuls/id/923508
* FRSIRT: ADV-2008-1940
http://www.frsirt.com/english/advisories/2008/1940/references
* SECTRACK: 1020382
http://www.securitytracker.com/id?1020382
* SECUNIA: 30857
http://secunia.com/advisories/30857
* XF: ie-location-locationhref-security-bypass(43366)
http://xforce.iss.net/xforce/xfdb/43366

CVE Reference:

CVE-2008-2947 (cve.mitre.org, nvd.nist.gov)

• 18152 HTML Element Cross-Domain Vulnerability (MS08-058/956390) (Remote File Checking)

A remote code execution or information disclosure vulnerability exists in Internet Explorer that could allow script to gain access to a browser window in another domain or Internet Explorer zone. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow remote code execution or information disclosure, depending on the operating system, if a user viewed the Web page.

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

References:

* MS: MS08-058
http://www.microsoft.com/technet/security/Bulletin/MS08-058.mspx
* SECUNIA: Microsoft Internet Explorer Multiple Vulnerabilities
http://secunia.com/advisories/30851/
* BID: Microsoft Internet Explorer HTML Element Cross Domain Security Bypass Vulnerability
http://www.securityfocus.com/bid/31615
* FRSIRT: FrSIRT/ADV-2008-2809
http://www.frsirt.com/english/advisories/2008/2809

CVE Reference:

CVE-2008-3472 (cve.mitre.org, nvd.nist.gov)

• 18153 Event Handling Cross-Domain Vulnerability (MS08-058/956390) (Remote File Checking)

A remote code execution or information disclosure vulnerability exists in Internet Explorer that could allow script to gain access to a browser window in another domain or Internet Explorer zone. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow remote code execution or information disclosure, depending on the operating system, if a user viewed the Web page.

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

References:

* MS: MS08-058
http://www.microsoft.com/technet/security/Bulletin/MS08-058.mspx
* SECUNIA: Microsoft Internet Explorer Multiple Vulnerabilities
http://secunia.com/advisories/30851/
* BID: Microsoft Internet Explorer Event Handling Cross Domain Security Bypass Vulnerability
http://www.securityfocus.com/bid/31616
* FRSIRT: FrSIRT/ADV-2008-2809
http://www.frsirt.com/english/advisories/2008/2809

CVE Reference:

CVE-2008-3473 (cve.mitre.org, nvd.nist.gov)

• 18154 Cross-Domain Information Disclosure Vulnerability (MS08-058/956390) (Remote File Checking)

An information disclosure vulnerability exists in Internet Explorer that could allow script to gain access to a browser window in another domain or Internet Explorer zone. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow information disclosure if a user viewed the Web page.

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

References:

* MS: MS08-058
http://www.microsoft.com/technet/security/Bulletin/MS08-058.mspx
* SECUNIA: Microsoft Internet Explorer Multiple Vulnerabilities
http://secunia.com/advisories/30851/
* BID: Microsoft Internet Explorer Cross Domain Information Disclosure Vulnerability
http://www.securityfocus.com/bid/31654
* FRSIRT: FrSIRT/ADV-2008-2809
http://www.frsirt.com/english/advisories/2008/2809

CVE Reference:

CVE-2008-3474 (cve.mitre.org, nvd.nist.gov)

• 18155 Uninitialized Memory Corruption Vulnerability (MS08-058/956390) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer accesses an object that has not been correctly initialized or that has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, 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.

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

References:

* MS: MS08-058
http://www.microsoft.com/technet/security/Bulletin/MS08-058.mspx
* SECUNIA: Microsoft Internet Explorer Multiple Vulnerabilities
http://secunia.com/advisories/30851/
* BID: Microsoft Internet Explorer Uninitialized Object Remote Memory Corruption Vulnerability
http://www.securityfocus.com/bid/31617
* FRSIRT: FrSIRT/ADV-2008-2809
http://www.frsirt.com/english/advisories/2008/2809

CVE Reference:

CVE-2008-3475 (cve.mitre.org, nvd.nist.gov)

• 18156 HTML Objects Memory Corruption Vulnerability (MS08-058/956390) (Remote File Checking)

A remote code execution vulnerability exists in Internet Explorer due to attempts to access uninitialized memory in certain situations. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, 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.

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

References:

* MS: MS08-058
http://www.microsoft.com/technet/security/Bulletin/MS08-058.mspx
* SECUNIA: Microsoft Internet Explorer Multiple Vulnerabilities
http://secunia.com/advisories/30851/
* BID: Microsoft Internet Explorer HTML Objects Uninitialized Memory Corruption Vulnerability
http://www.securityfocus.com/bid/31618
* FRSIRT: FrSIRT/ADV-2008-2809
http://www.frsirt.com/english/advisories/2008/2809

CVE Reference:

CVE-2008-3476 (cve.mitre.org, nvd.nist.gov)

• 18158 Calendar Object Validation Vulnerability (MS08-057/956416) (Remote File Checking)

A remote code execution vulnerability exists in the way Excel processes a VBA Performance Cache. The vulnerability could allow remote code execution if a user opens a specially crafted Excel file in a VBA Performance Cache. 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: MS08-057
http://www.microsoft.com/technet/security/Bulletin/MS08-057.mspx
* SECUNIA: Microsoft Excel Multiple Vulnerabilities
http://secunia.com/advisories/32211/
* BID: Microsoft Excel Calendar Object Validation Remote Code Execution Vulnerability
http://www.securityfocus.com/bid/31702
* FRSIRT: FrSIRT/ADV-2008-2808
http://www.frsirt.com/english/advisories/2008/2808

CVE Reference:

CVE-2008-3477 (cve.mitre.org, nvd.nist.gov)

• 18159 File Format Parsing Vulnerability (MS08-057/956416) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Excel as a result of improper memory allocation when loading Excel objects. The vulnerability could allow remote code execution if a user opens a specially crafted Excel file that includes a malformed object. 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: MS08-057
http://www.microsoft.com/technet/security/Bulletin/MS08-057.mspx
* SECUNIA: Microsoft Excel Multiple Vulnerabilities
http://secunia.com/advisories/32211/
* BID: Microsoft Excel BIFF File Format Parsing Remote Code Execution Vulnerability
http://www.securityfocus.com/bid/31705
* FRSIRT: FrSIRT/ADV-2008-2808
http://www.frsirt.com/english/advisories/2008/2808

CVE Reference:

CVE-2008-3471 (cve.mitre.org, nvd.nist.gov)

• 18160 Formula Parsing Vulnerability (MS08-057/956416) (Remote File Checking)

The specific flaw exists when parsing Microsoft Excel documents containing a specially crafted formula embedded inside a cell. This can result in a remote compromise of the system under the context of the currently logged in user.

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

References:

* MS: MS08-057
http://www.microsoft.com/technet/security/Bulletin/MS08-057.mspx
* SECUNIA: Microsoft Excel Multiple Vulnerabilities
http://secunia.com/advisories/32211/
* BID: Microsoft Excel Formula Parsing Remote Code Execution Vulnerability
http://www.securityfocus.com/bid/31706
* FRSIRT: FrSIRT/ADV-2008-2808
http://www.frsirt.com/english/advisories/2008/2808

CVE Reference:

CVE-2008-4019 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2008-3471 Microsoft CVSS 2.0 Score = 10.0**

Microsoft Excel 2000 SP3, 2002 SP3, 2003 SP2 and SP3, and 2007 Gold and SP1; Office Excel Viewer 2003 SP3; Office Excel Viewer; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Gold and SP1; Office 2004 and 2008 for Mac; and Open XML File Format Converter for Mac do not properly allocate memory when loading Excel objects during parsing of the Excel spreadsheet file format, which allows remote attackers to execute arbitrary code via a crafted BIFF file, aka "File Format Parsing Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS08-057.mspx

CVE Reference: CVE-2008-3471

- **CVE-2008-3479 Microsoft CVSS 2.0 Score = 10.0**

The Microsoft Message Queuing (MSMQ) service in Microsoft Windows 2000 SP4 does not properly validate parameters to string APIs, which allows remote attackers to execute arbitrary code via a crafted RPC call that overflows a "heap request," aka "Message Queuing Service Remote Code Execution Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS08-065.mspx

CVE Reference: CVE-2008-3479

- **CVE-2008-4023 Microsoft CVSS 2.0 Score = 10.0**

Active Directory in Microsoft Windows 2000 SP4 does not properly allocate memory for (1) LDAP and (2) LDAPS requests, which allows remote attackers to execute arbitrary code via a crafted request, aka "Active Directory Overflow Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS08-060.mspx

CVE Reference: CVE-2008-4023

- **CVE-2008-4038 Microsoft CVSS 2.0 Score = 10.0**

Buffer underflow in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to execute arbitrary code via a Server Message Block (SMB) request that contains a filename with a crafted length, aka "SMB Buffer Underflow Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS08-063.mspx

CVE Reference: CVE-2008-4038

- **CVE-2008-3472 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 6 and 7 does not properly determine the domain or security zone of origin of web script, which allows remote attackers to bypass the intended cross-domain security policy, and execute arbitrary code or obtain sensitive information, via a crafted HTML document, aka "HTML Element Cross-Domain Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS08-058.mspx

CVE Reference: CVE-2008-3472

- **CVE-2008-3473 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 6 and 7 does not properly determine the domain or security zone of origin of web script, which allows remote attackers to bypass the intended cross-domain security policy, and execute arbitrary code or obtain sensitive information, via a crafted HTML document, aka "Event Handling Cross-Domain Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS08-058.mspx

CVE Reference: CVE-2008-3473

- **CVE-2008-3475 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 6 does not properly handle errors associated with access to an object that has been (1) incorrectly initialized or (2) deleted, which allows remote attackers to execute arbitrary code via a crafted HTML document, aka "Uninitialized Memory Corruption Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS08-058.mspx

CVE Reference: CVE-2008-3475

- **CVE-2008-3476 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 5.01 SP4 and 6 does not properly handle errors associated with access to uninitialized memory, which allows remote attackers to execute arbitrary code via a crafted HTML document, aka "HTML Objects Memory Corruption Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS08-058.mspx

CVE Reference: CVE-2008-3476

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