ScoutNews
The weekly Security update from the makers of SecureScout
February 12, 2010

2010 Issue #7

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

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

Bob Russo on PCI compliance. N.Y. town goes after bank for online theft. ID theft on the rise. New trojan harvesting credentials.

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

- **PCI compliance: What it is and why it matters (Q&A)**

Bob Russo, general manager of the PCI Security Standards Council.

(Credit: PCI Security Standards Council)

If you own a bank account or use credit cards, chances are you've heard the term "PCI compliant." But you probably don't know what it means. Cnet Security

Full Story :
http://news.cnet.com/8301-27080_3-10448197-245.html?part=rss&subj=news&tag=2547-1_3-0-20

- **Poughkeepsie, N.Y., slams bank for $378,000 online theft**

Computerworld - The theft of $378,000 from the town of Poughkeepsie, N.Y., is prompting questions about the responsibility of banks to protect customer accounts from online criminals.

In a statement last week, a Poughkeepsie town official revealed that thieves had broken into the town's TD Bank NA account and transferred $378,000 to accounts in the Ukraine.

The thefts took place over a two-day period in mid-January during which a total of nine attempts were made to steal money. In the end, four of the attempts were successful, resulting in the lost money. Computerworld

Full Story :
http://www.computerworld.com/s/article/9153598/Poughkeepsie_N.Y._slams_bank_for_378_000_online_theft?source

- **ID theft still on the rise, but victims respond faster**

Incidents of identity fraud and the total cost of fraud once again climbed last year, but consumers are becoming better equipped to respond to the occurrences of theft, according to a report released Wednesday by Javelin Strategy & Research.

The seventh annual "2010 Identity Fraud Survey Report," which polled more than 5,000 U.S. consumers, concluded that the number of victims rose to 11.1 million adults in 2009, an increase of 12 percent. Meanwhile, the total annual fraud amount experienced by these victims jumped 12.5 percent to $54 billion.

This is the second straight year that both of those statistics have risen. SC Magazine

Full Story :
http://www.scmagazineus.com/id-theft-still-on-the-rise-but-victims-respond-faster/article/163548/?utm_source=feedb

- **New "Bugat" trojan harvesting banking credentials**

Researchers discovered a new banking trojan that is being used to steal the financial credentials of customers at approximately 15 large- and mid-size U.S. banks.

The "Bugat" trojan, discovered by SecureWorks researchers in January, has capabilities similar to the notorious data-stealing trojans Clampi and Zeus, Jason Milletary, security researcher with SecureWorks' research team, the Counter Threat Unit (CTU), told SCMagazineUS.com on Tuesday.

The malware monitors an infected user's web browsing activity and searches for the URLs of more than a dozen financial institutions, Milletary said. When a user accesses one of the targeted URLs, the trojan captures account credentials and sends them back to the criminal's remote server. SC Magazine

Full Story :
http://www.scmagazineus.com/new-bugat-trojan-harvesting-banking-credentials/article/163458/?utm_source=feedbu

New Vulnerabilities Tested in SecureScout

- **18695 ICMPv6 Router Advertisement Vulnerability (MS10-009/974145) (Remote File Checking)**

A remote code execution vulnerability exists in the Windows TCP/IP stack due to insufficient bounds checking when processing specially crafted ICMPv6 Router Advertisement packets. An anonymous attacker could exploit the vulnerability by sending specially crafted ICMPv6 Router Advertisement packets to a computer with IPv6 enabled. 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: MS10-009
http://www.microsoft.com/technet/security/Bulletin/MS10-009.mspx
* BID: 38061
http://www.securityfocus.com/bid/38061
* SECTRACK: 1023561
http://securitytracker.com/alerts/2010/Feb/1023561.html
* VUPEN: VUPEN/ADV-2010-0342
http://www.vupen.com/english/advisories/2010/0342

CVE Reference:

CVE-2010-0239 (cve.mitre.org, nvd.nist.gov)

• 18696 Header MDL Fragmentation Vulnerability (MS10-009/974145) (Remote File Checking)

A remote code execution vulnerability exists in the Windows TCP/IP stack due to the manner in which the TCP/IP stack handles specially crafted Encapsulating Security Payloads (ESP) over UDP datagram fragments when running a custom network driver. 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: MS10-009
http://www.microsoft.com/technet/security/Bulletin/MS10-009.mspx
* BID: 38062
http://www.securityfocus.com/bid/38062
* SECTRACK: 1023561
http://securitytracker.com/alerts/2010/Feb/1023561.html
* VUPEN: VUPEN/ADV-2010-0342
http://www.vupen.com/english/advisories/2010/0342

CVE Reference:

CVE-2010-0240 (cve.mitre.org, nvd.nist.gov)

• 18697 ICMPv6 Route Information Vulnerability (MS10-009/974145) (Remote File Checking)

A remote code execution vulnerability exists in the Windows TCP/IP stack due to insufficient bounds checking when processing specially crafted ICMPv6 Route Information packets. An anonymous attacker could exploit the vulnerability by sending specially crafted ICMPv6 Route Information packets to a computer with IPv6 enabled. 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: MS10-009
http://www.microsoft.com/technet/security/Bulletin/MS10-009.mspx
* BID: 38063
http://www.securityfocus.com/bid/38063
* SECTRACK: 1023561
http://securitytracker.com/alerts/2010/Feb/1023561.html
* VUPEN: VUPEN/ADV-2010-0342
http://www.vupen.com/english/advisories/2010/0342

CVE Reference:

CVE-2010-0241 (cve.mitre.org, nvd.nist.gov)

• 18698 TCP/IP Selective Acknowledgment Vulnerability (MS10-009/974145) (Remote File Checking)

A denial of service vulnerability exists in TCP/IP processing in Microsoft Windows due to an error in the processing of specially crafted TCP packets with a malformed selective acknowledgment (SACK) value. An attacker could exploit the vulnerability by sending the target system a small number of specially crafted packets causing the affected system to stop responding and automatically restart.

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

References:

* MS: MS10-009
http://www.microsoft.com/technet/security/Bulletin/MS10-009.mspx
* BID: 38064
http://www.securityfocus.com/bid/38064
* SECTRACK: 1023561
http://securitytracker.com/alerts/2010/Feb/1023561.html
* VUPEN: VUPEN/ADV-2010-0342
http://www.vupen.com/english/advisories/2010/0342

CVE Reference:

CVE-2010-0242 (cve.mitre.org, nvd.nist.gov)

- **18699 SMB Client Pool Corruption Vulnerability (MS10-006/978251) (Remote File Checking)**

An unauthenticated remote code execution vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB responses. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted SMB response to a client-initiated SMB request. An attacker who successfully exploited this vulnerability could take complete control of the system.

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

References:

* MS: MS10-006
http://www.microsoft.com/technet/security/Bulletin/MS10-006.mspx
* BID: 38093
http://www.securityfocus.com/bid/38093
* SECTRACK: 1023559
http://securitytracker.com/alerts/2010/Feb/1023559.html
* VUPEN: VUPEN/ADV-2010-0339
http://www.vupen.com/english/advisories/2010/0339

CVE Reference:

CVE-2010-0016 (cve.mitre.org, nvd.nist.gov)

- **18700 SMB Client Race Condition Vulnerability (MS10-006/978251) (Remote File Checking)**

An unauthenticated remote code execution vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB packets. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted SMB response to client-initiated SMB request. An attacker who successfully exploited this vulnerability could take complete control of the system.

On Windows Vista and Windows Server 2008, this vulnerability could result in an elevation of privilege vulnerability due to the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB negotiate responses. An attacker who successfully exploited this vulnerability could run arbitrary code with system-level privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker must have valid logon credentials and be able to log on locally to elevate privileges in this manner.

This vulnerability could also result in a denial of service. An attempt to exploit the vulnerability in this manner would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted SMB response to a client-initiated SMB request. An attacker who successfully exploited this vulnerability could cause the computer to stop responding until restarted.

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

References:

* MS: MS10-006
http://www.microsoft.com/technet/security/Bulletin/MS10-006.mspx
* BID: 38100
http://www.securityfocus.com/bid/38100
* SECTRACK: 1023559
http://securitytracker.com/alerts/2010/Feb/1023559.html
* VUPEN: VUPEN/ADV-2010-0339
http://www.vupen.com/english/advisories/2010/0339

CVE Reference:

CVE-2010-0017 (cve.mitre.org, nvd.nist.gov)

- **18701 SMB Pathname Overflow Vulnerability (MS10-012/971468) (Remote File Checking)**

An authenticated remote code execution vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB packets. An attacker could exploit the vulnerability by sending a specially crafted network message to a system running the Server service as an authenticated user. While an attacker who successfully exploited this vulnerability could take complete control of the affected system, attempts to exploit this vulnerability will most probably result in a Denial of Service condition.

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

References:

* MS: MS10-012
http://www.microsoft.com/technet/security/Bulletin/MS10-012.mspx
* BID: 38049
http://www.securityfocus.com/bid/38049
* SECTRACK: 1023568
http://securitytracker.com/alerts/2010/Feb/1023568.html
* VUPEN: VUPEN/ADV-2010-0345
http://www.vupen.com/english/advisories/2010/0345

CVE Reference:

CVE-2010-0020 (cve.mitre.org, nvd.nist.gov)

• 18702 SMB Memory Corruption Vulnerability (MS10-012/971468) (Remote File Checking)

A denial of service vulnerability exists in the way that in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB packets. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a computer running the Server service.

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

References:

* MS: MS10-012
http://www.microsoft.com/technet/security/Bulletin/MS10-012.mspx
* BID: 38054
http://www.securityfocus.com/bid/38054
* SECTRACK: 1023568
http://securitytracker.com/alerts/2010/Feb/1023568.html
* VUPEN: VUPEN/ADV-2010-0345
http://www.vupen.com/english/advisories/2010/0345

CVE Reference:

CVE-2010-0021 (cve.mitre.org, nvd.nist.gov)

• 18703 SMB Null Pointer Vulnerability (MS10-012/971468) (Remote File Checking)

A denial of service vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB (SMB) packets. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted network message to a computer running the Server service. An attacker who successfully exploited this vulnerability could cause the computer to stop responding until restarted.

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

References:

* MS: MS10-012
http://www.microsoft.com/technet/security/Bulletin/MS10-012.mspx
* BID: 38051
http://www.securityfocus.com/bid/38051
* SECTRACK: 1023568
http://securitytracker.com/alerts/2010/Feb/1023568.html
* VUPEN: VUPEN/ADV-2010-0345
http://www.vupen.com/english/advisories/2010/0345

CVE Reference:

CVE-2010-0022 (cve.mitre.org, nvd.nist.gov)

• 18704 SMB NTLM Authentication Lack of Entropy Vulnerability (MS10-012/971468) (Remote File Checking)

An unauthenticated elevation of privilege vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles authentication attempts. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending large amounts of authentication requests to the SMB server. An attacker who successfully exploited this vulnerability could access the SMB service on the target user under the credentials of an authorized user.

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

References:

* MS: MS10-012
http://www.microsoft.com/technet/security/Bulletin/MS10-012.mspx
* BID: 38085
http://www.securityfocus.com/bid/38085
* SECTRACK: 1023568
http://securitytracker.com/alerts/2010/Feb/1023568.html
* VUPEN: VUPEN/ADV-2010-0345
http://www.vupen.com/english/advisories/2010/0345

CVE Reference:

CVE-2010-0231 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2010-0231 Microsoft CVSS 2.0 Score = 10.0**

The SMB implementation in the Server service in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not use a sufficient source of entropy, which allows remote attackers to obtain access to files and other SMB resources via a large number of authentication requests, related to server-generated challenges, certain "duplicate values," and spoofing of an authentication token, aka "SMB NTLM Authentication Lack of Entropy Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS10-012.mspx

CVE Reference: CVE-2010-0231

- **CVE-2010-0239 Microsoft CVSS 2.0 Score = 10.0**

The TCP/IP implementation in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2, when IPv6 is enabled, does not properly perform bounds checking on ICMPv6 Router Advertisement packets, which allows remote attackers to execute arbitrary code via crafted packets, aka "ICMPv6 Router Advertisement Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS10-009.mspx

CVE Reference: CVE-2010-0239

- **CVE-2010-0240 Microsoft CVSS 2.0 Score = 10.0**

The TCP/IP implementation in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2, when a custom network driver is used, does not properly handle local fragmentation of Encapsulating Security Payload (ESP) over UDP packets, which allows remote attackers to execute arbitrary code via crafted packets, aka "Header MDL Fragmentation Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS10-009.mspx

CVE Reference: CVE-2010-0240

- **CVE-2010-0241 Microsoft CVSS 2.0 Score = 10.0**

The TCP/IP implementation in Microsoft Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2, when IPv6 is enabled, does not properly perform bounds checking on ICMPv6 Route Information packets, which allows remote attackers to execute arbitrary code via crafted packets, aka "ICMPv6 Route Information Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS10-009.mspx

CVE Reference: CVE-2010-0241

- **CVE-2010-0243 Microsoft CVSS 2.0 Score = 10.0**

Buffer overflow in MSO.DLL in Microsoft Office XP SP3 and Office 2004 for Mac allows remote attackers to execute arbitrary code via a crafted Office document, aka "MSO.DLL Buffer Overflow."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS10-003.mspx

CVE Reference: CVE-2010-0243

- **CVE-2010-0016 Microsoft CVSS 2.0 Score = 9.3**

The SMB client implementation in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not properly validate response fields, which allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code via a crafted response, aka "SMB Client Pool Corruption Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS10-006.mspx

CVE Reference: CVE-2010-0016

- **CVE-2010-0017 Microsoft CVSS 2.0 Score = 9.3**

Race condition in the SMB client implementation in Microsoft Windows Server 2008 R2 and Windows 7 allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code, and in the SMB client implementation in Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2 allows local users to gain privileges, via a crafted SMB Negotiate response, aka "SMB Client Race Condition Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS10-006.mspx

CVE Reference: CVE-2010-0017

- **CVE-2010-0028 Microsoft CVSS 2.0 Score = 9.3**

Integer overflow in Microsoft Paint in Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 allows remote attackers to execute arbitrary code via a crafted JPEG (.JPG) file, aka "MS Paint Integer Overflow Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS10-005.mspx

SECUNIA: http://secunia.com/advisories/36634

CVE Reference: CVE-2010-0028

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