

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

[Messenger Service Vulnerability Scanner](#) - The S4 Messenger Service 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 Microsoft Windows Messenger Service flaw (MS03-043).

Download Here:

<http://www.netvigilance.com/productdownloads?productname=messengerservicevulnerabilityscanner>

This Week in Review

PCI gives out new getting started checklist. Keyboard strokes sniffed from electronic waves. Google sparks privacy concerns. Web malware against the energy sector.

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

• Befuddled companies get checklist for complying with PCI security standard

March 9, 2009 (Computerworld) The organization responsible for administering the Payment Card Industry Data Security Standard is offering new guidance to companies on how to focus their PCI DSS compliance efforts so as to more quickly them in position to meet the rules on protecting credit and debit card data.

Bob Russo, the council's general manager, said the framework is "the culmination of a lot of input" from various stakeholders within the payment card industry. It's designed, he added, to help companies that haven't yet to start on their PCI compliance efforts and are wondering what they should do first.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9129277&source=rss_topic1

• Researchers sniff PC keyboard strokes from thin air

March 12, 2009 (IDG News Service) That PC keyboard you're using may be giving away your passwords. Researchers say they've discovered new ways to read what you're typing by aiming special wireless or laser equipment at the keyboard or by simply plugging into a nearby electrical socket.

The Ecole Polytechnique team did its work over the air. Using an oscilloscope and an inexpensive wireless antenna, the team was able to pick up keystrokes from virtually any keyboard, including laptops. "We discovered four different ways to recover the keystroke of a keyboard," said Matin Vuagnoux, a Ph.D. student at the university. With the keyboard's cabling and nearby power wires acting as antennas for these electromagnetic signals, the researchers were able to read keystrokes with 95% accuracy over a distance of up to 20 meters (22 yards), in ideal conditions.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9129575&source=rss_topic1

• **Google's interest-based advertising sparks privacy debate**

Google on Wednesday launched an "interest-based" advertising service, sparking a larger discussion among privacy-advocacy groups over data collection concerns.

Based on the type of websites users visit, Google will place users into interest categories -- such as sports, cars and cats -- and serve ads related to these categories, Nicole Wong, deputy general counsel at Google, told SCMagazineUS.com Thursday. Users will have the option of modifying the interest categories they fall into or "opt-out" by downloading a browser plug-in, which permanently stores the user's preference for opting out of interest-based ads.

Companies including Yahoo, AOL and Microsoft have been using interest-based advertising for up to 10 years, Wong said. But, typically, there has been a lack of transparency and choice for users -- which Google has worked to mitigate in developing its own program.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Googles-interest-based-advertising-sparks-privacy-debate/article/128707/>

• **Web malware, more advanced and targeted than ever**

End-users working in the energy-and-oil sector are most at-risk to succumbing to web malware, according to ScanSafe's annual threat report released this week.

Based on an analysis of 200 billion web requests processed by the security company on behalf of its worldwide customer base, the top five verticals most susceptible to web malware infection were energy and oil, pharmaceutical and chemical, engineering and construction, transportation and shipping and travel and entertainment.

Mary Landesman, ScanSafe's senior security researcher, told SCMagazineUS.com on Wednesday that this is likely attributable to the vast amounts of intellectual property stored by those sectors. Thus, an attacker who can steal data may be able to handsomely profit by, say, selling the goods to a competitor.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Web-malware-more-advanced-and-targeted-than-ever/article/128712/>

New Vulnerabilities Tested in SecureScout

• **18287 Windows Kernel Input Validation Vulnerability (MS09-006/958690) (Remote File Checking)**

A remote code execution vulnerability exists in the Windows kernel due to improper validation of input passed from user mode through the kernel component of GDI. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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: MS09-006

<http://www.microsoft.com/technet/security/bulletin/MS09-006.mspx>

* BID: 34012

<http://www.securityfocus.com/bid/34012>

* SECUNIA: 34117
<http://secunia.com/advisories/34117/>

CVE Reference:

CVE-2009-0081 (cve.mitre.org, nvd.nist.gov)

• **18292 Windows Kernel Handle Validation Vulnerability (MS09-006/958690) (Remote File Checking)**

An elevation of privilege vulnerability exists in the Windows kernel due to the manner in which the kernel validates handles. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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: MS09-006
<http://www.microsoft.com/technet/security/bulletin/MS09-006.msp>
* BID: 34027
<http://www.securityfocus.com/bid/34027>
* SECUNIA: 34117
<http://secunia.com/advisories/34117/>

CVE Reference:

CVE-2009-0082 (cve.mitre.org, nvd.nist.gov)

• **18293 Windows Kernel Invalid Pointer Vulnerability (MS09-006/958690) (Remote File Checking)**

An elevation of privilege vulnerability exists in the Windows kernel due to improper handling of a specially crafted invalid pointer. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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: MS09-006
<http://www.microsoft.com/technet/security/bulletin/MS09-006.msp>
* BID: 34025
<http://www.securityfocus.com/bid/34025>
* SECUNIA: 34117
<http://secunia.com/advisories/34117/>

CVE Reference:

CVE-2009-0083 (cve.mitre.org, nvd.nist.gov)

• **18294 SChannel Spoofing Vulnerability (MS09-007/960225) (Remote File Checking)**

A spoofing vulnerability exists in the Microsoft Windows SChannel authentication component when using certificate based authentication. An attacker who successfully exploited this vulnerability would be able to authenticate to a server using only an authorized user's digital certificate and without the associated private key.

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

References:

* MS: MS09-007
<http://www.microsoft.com/technet/security/bulletin/MS09-007.msp>
* BID: 34015
<http://www.securityfocus.com/bid/34015>
* SECUNIA: 34215
<http://secunia.com/advisories/34215/>

CVE Reference:

CVE-2009-0085 (cve.mitre.org, nvd.nist.gov)

• **18295 DNS Server Query Validation Vulnerability (MS09-008/962238) (Remote File Checking)**

A spoofing vulnerability exists in Windows DNS server. This vulnerability could allow a remote unauthenticated attacker to quickly and reliably spoof responses and insert records into the DNS server's cache, thereby redirecting Internet traffic.

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

References:

- * MS: MS09-008
<http://www.microsoft.com/technet/security/bulletin/MS09-008.msp>
- * BID: 33982
<http://www.securityfocus.com/bid/33982>
- * SECUNIA: 34217
<http://secunia.com/advisories/34217/>

CVE Reference:

CVE-2009-0233 (cve.mitre.org, nvd.nist.gov)

• 18296 DNS Server Response Validation Vulnerability (MS09-008/962238) (Remote File Checking)

A response validation vulnerability exists in Windows DNS Server. The vulnerability could allow an unauthenticated remote attacker to send specially crafted queries to a DNS server so as to allow greater predictability of transaction IDs used by the DNS server and thus to redirect Internet traffic from legitimate locations.

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

References:

- * MS: MS09-008
<http://www.microsoft.com/technet/security/bulletin/MS09-008.msp>
- * BID: 33988
<http://www.securityfocus.com/bid/33988>
- * SECUNIA: 34217
<http://secunia.com/advisories/34217/>

CVE Reference:

CVE-2009-0234 (cve.mitre.org, nvd.nist.gov)

• 18297 DNS Server Vulnerability in WPAD Registration Vulnerability (MS09-008/962238) (Remote File Checking)

A man-in-the-middle attack vulnerability exists in Windows DNS servers where dynamic update is used and ISATAP and WPAD are not already registered in DNS. This vulnerability could allow a remote authenticated attacker to spoof a web proxy thereby redirect Internet traffic to an address of the attacker's choice.

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

References:

- * MS: MS09-008
<http://www.microsoft.com/technet/security/bulletin/MS09-008.msp>
- * BID: 33989
<http://www.securityfocus.com/bid/33989>
- * SECUNIA: 34217
<http://secunia.com/advisories/34217/>

CVE Reference:

CVE-2009-0093 (cve.mitre.org, nvd.nist.gov)

• 18298 WPAD WINS Server Registration Vulnerability (MS09-008/962238) (Remote File Checking)

A man-in-the-middle attack vulnerability exists in Windows WINS servers. This vulnerability could allow a remote authenticated attacker to spoof a web proxy and thereby redirect Internet traffic to an address of the attacker's choice.

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

References:

- * MS: MS09-008
<http://www.microsoft.com/technet/security/bulletin/MS09-008.msp>
- * BID: 34013
<http://www.securityfocus.com/bid/34013>
- * SECUNIA: 34217
<http://secunia.com/advisories/34217/>

CVE Reference:

CVE-2009-0094 (cve.mitre.org, nvd.nist.gov)

• 18299 BIND DSA_do_verify() return check Vulnerability

BIND 9.3.x up to 9.3.6, 9.4.x up to 9.4.3, 9.5.x up to 9.5.1 and 9.6.0, do not properly check the return value from the OpenSSL DSA_verify function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature.

The vulnerability has been fixed in versions 9.3.6-P1, 9.4.3-P1, 9.5.1-P1, 9.6.0-P1.

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

References:

- * BUGTRAQ: 20090120 rPSA-2009-0009-1 bind bind-utils
<http://www.securityfocus.com/archive/1/archive/1/500207/100/0/threaded>
- * MISC:
<http://www.ocert.org/advisories/ocert-2008-016.html>
- * MISC:
http://groups.google.com/group/comp.protocols.dns.bind/browse_thread/thread/49ef622c8329fd33
- * CONFIRM:
<http://wiki.rpath.com/Advisories:rPSA-2009-0009>
- * CONFIRM:
<https://issues.rpath.com/browse/RPL-2938>
- * CONFIRM:
<https://www.isc.org/node/373>
- * CONFIRM:
http://www.openbsd.org/errata44.html#008_bind
- * CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2009-045.htm>
- * FEDORA: FEDORA-2009-0350
<https://www.redhat.com/archives/fedora-package-announce/2009-January/msg00393.html>
- * FREEBSD: FreeBSD-SA-09:04
<http://security.freebsd.org/advisories/FreeBSD-SA-09:04.bind.asc>
- * SLACKWARE: SSA:2009-014-02
http://slackware.com/security/viewer.php?l=slackware-security&y=2009&m=slackware-security_540362
- * SUNALERT: 250846
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-250846-1>
- * NETVIGILANCE-UNKNOWN: ADV-2009-0043
<http://www.frsirt.com/english/advisories/2009/0043>
- * NETVIGILANCE-UNKNOWN: ADV-2009-0366
<http://www.frsirt.com/english/advisories/2009/0366>
- * SECUNIA: 33559
<http://secunia.com/advisories/33559>
- * SECUNIA: 33683
<http://secunia.com/advisories/33683>
- * SECUNIA: 33494
<http://secunia.com/advisories/33494>
- * SECUNIA: 33546
<http://secunia.com/advisories/33546>
- * SECUNIA: 33551
<http://secunia.com/advisories/33551>
- * SECUNIA: 33882
<http://secunia.com/advisories/33882>

CVE Reference:

CVE-2009-0025 (cve.mitre.org, nvd.nist.gov)

• 18300 BIND EVP_VerifyFinal() return check Vulnerability

BIND 9.3.x up to 9.3.6, 9.4.x up to 9.4.3, 9.5.x up to 9.5.1 and 9.6.0, do not properly check the return value from the OpenSSL EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature.

The vulnerability has been fixed in versions 9.3.6-P1, 9.4.3-P1, 9.5.1-P1, 9.6.0-P1.

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

References:

- * MISC:
http://groups.google.com/group/comp.protocols.dns.bind/browse_thread/thread/49ef622c8329fd33
- * CONFIRM:

<https://www.isc.org/node/373>

* MANDRIVA: MDVSA-2009:037

<http://www.mandriva.com/security/advisories?name=MDVSA-2009:037>

* SLACKWARE: SSA:2009-014-02

<http://slackware.com/security/viewer.php?l=slackware-security&y=2009&m=slackware-security.540362>

* NETVIGILANCE-UNKNOWN: ADV-2009-0043

<http://www.frsirt.com/english/advisories/2009/0043>

* SECUNIA: 33559

<http://secunia.com/advisories/33559>

CVE Reference:

CVE-2009-0265 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2009-0081 Microsoft CVSS 2.0 Score = 9.3**

The graphics device interface (GDI) implementation in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly validate input received from user mode, which allows remote attackers to execute arbitrary code via a crafted (1) Windows Metafile (aka WMF) or (2) Enhanced Metafile (aka EMF) image file, aka "Windows Kernel Input Validation Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-006.mspx>

CVE Reference: [CVE-2009-0081](#)

• **CVE-2009-0082 Microsoft CVSS 2.0 Score = 7.2**

The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly validate handles, which allows local users to gain privileges via a crafted application that triggers unspecified "actions," aka "Windows Kernel Handle Validation Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-006.mspx>

CVE Reference: [CVE-2009-0082](#)

• **CVE-2009-0083 Microsoft CVSS 2.0 Score = 7.2**

The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 does not properly handle invalid pointers, which allows local users to gain privileges via an application that triggers use of a crafted pointer, aka "Windows Kernel Invalid Pointer Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-006.mspx>

CVE Reference: [CVE-2009-0083](#)

• **CVE-2009-0085 Microsoft CVSS 2.0 Score = 7.1**

The Secure Channel (aka SChannel) authentication component in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008, when certificate authentication is used, does not properly validate the client's key exchange data in Transport Layer Security (TLS) handshake messages, which allows remote attackers to spoof authentication by crafting a TLS packet based on knowledge of the certificate but not the private key, aka "SChannel Spoofing Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-007.mspx>

CVE Reference: [CVE-2009-0085](#)

• **CVE-2009-0234 Microsoft CVSS 2.0 Score = 6.4**

The DNS Resolver Cache Service (aka DNSCache) in Windows DNS Server in Microsoft Windows 2000 SP4, Server 2003 SP1 and SP2, and Server 2008 does not properly cache crafted DNS responses, which makes it easier for remote attackers to predict transaction IDs and poison caches by sending many crafted DNS queries that trigger "unnecessary lookups," aka "DNS Server Response Validation Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-008.msp>

CVE Reference: [CVE-2009-0234](#)

• **CVE-2009-0233 Microsoft CVSS 2.0 Score = 5.8**

The DNS Resolver Cache Service (aka DNSCache) in Windows DNS Server in Microsoft Windows 2000 SP4, Server 2003 SP1 and SP2, and Server 2008, when dynamic updates are enabled, does not reuse cached DNS responses in all applicable situations, which makes it easier for remote attackers to predict transaction IDs and poison caches by simultaneously sending crafted DNS queries and responses, aka "DNS Server Query Validation Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-008.msp>

CVE Reference: [CVE-2009-0233](#)

• **CVE-2009-0537 Microsoft CVSS 2.0 Score = 4.9**

Integer overflow in the fts_build function in fts.c in libc in (1) OpenBSD 4.4 and earlier and (2) Microsoft Interix 6.0 build 10.0.6030.0 allows context-dependent attackers to cause a denial of service (application crash) via a deep directory tree, related to the fts_level structure member, as demonstrated by (a) du, (b) rm, (c) chmod, and (d) chgrp on OpenBSD; and (e) SearchIndexer.exe on Vista Enterprise.

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

References:

BID: <http://www.securityfocus.com/bid/34008>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/501505/100/0/threaded>

CONFIRM: <http://www.openbsd.org/cgi-bin/cvsweb/src/lib/libc/gen/fts.c.diff?r1=1.41;r2=1.42;f=h>

CONFIRM: <http://www.openbsd.org/cgi-bin/cvsweb/src/lib/libc/gen/fts.c>

MILWORM: <http://www.milw0rm.com/exploits/8163>

SREASONRES: http://securityreason.com/achievement_securityalert/60

CVE Reference: [CVE-2009-0537](#)

• **CVE-2009-0094 Microsoft CVSS 2.0 Score = 4.0**

The WINS server in Microsoft Windows 2000 SP4 and Server 2003 SP1 and SP2 does not restrict registration of the (1) "wpad" and (2) "isatap" NetBIOS names, which allows remote authenticated users to hijack the Web Proxy Auto-Discovery (WPAD) and Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) features, and conduct man-in-the-middle attacks by spoofing a proxy server or ISATAP route, by registering one of these names in the WINS database, aka "WPAD WINS Server Registration Vulnerability," a related issue to CVE-2007-1692. Per: <http://www.microsoft.com/technet/security/Bulletin/MS09-008.msp> Mitigating Factors for WPAD WINS Server Registration Vulnerability - CVE-2009-0094 Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation. If WINS server already has WPAD and ISATAP registered than an attacker will not be able to register these as well.

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-008.msp>

CVE Reference: [CVE-2009-0094](#)

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