ScoutNews
The weekly Security update from the makers of SecureScout
June 19, 2009

2009 Issue #25

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

WinHoneyd v1.1.1 - Download WinHoneyd executable package by filling our download form. Size: 2384KB

Download Here:
http://www.netvigilance.com/productdownloads?productname=winhoneyd-1.1.1.zip

This Week in Review

Iran leaders trying to cut off protesters. A look at what a security policy should consist of. New way of protecting data. Criminal network revealed.

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

- **Iran's leaders fight Internet; Internet wins (so far)**

Computerworld - Iran's government in recent days has tried to cut off Internet access for most of its election protestors by shutting down routers at the nation's perimeters, ripping satellite dishes off roofs, cutting cables and turning off telephone switching networks.

One cybersecurity expert, Stephen Spoonamore, a partner at Global Strategic Partners LLC in Washington, pointed out that at about the same time Iran was trying shut down phone and switching systems this weekend -- a response to the huge crowds of citizens upset by what they see as a stolen presidential election -- electric power was lost in Tehran.

He believes that once the Iranians began turning off switches to the nation's phone networks, IP-enabled pieces of its electric grid didn't get commands they expected. When you lose switching, "you end up with systems going down that you didn't expect to go down," he said.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9134471

- **How to Write an Information Security Policy**

CSO - An Information Security Policy is the cornerstone of an Information Security Program. It should reflect the organization's objectives for security and the agreed upon management strategy for securing information.

In order to be useful in providing authority to execute the remainder of the Information Security Program, it must also be formally agreed upon by executive management. This means that, in order to compose an information security policy document, an organization has to have well-defined objectives for security and an agreed-upon management strategy for securing information. If there is debate over the content of the policy, then the debate will continue throughout subsequent attempts to enforce it, with the consequence that the Information Security Program itself will be dysfunctional.

Also see CSOonline.com's IT Security Management: The Basics Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9134451

- **PCI compliance strategy calls for hiding card data in plain sight**

Network World - Direct-marketing retailer Fingerhut is undertaking a new strategy to protect sensitive payment-card information: Hiding it in plain sight through a data-scrambling method called “tokenization.”

Fingerhut's manager of information security Mark Lieberg says the strategy involves replacing the credit card number in the database where it’s stored with a different number that’s not related. To carry out this process, called “tokenization,” Fingerhut is adding nuBridges' Protect software for encryption so the real card data is stored securely but a substitute is created when card data needs to be shared across Fingerhut’s network for any number of reasons. Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9134559

- **Criminal network to trade botnets and malware uncovered**

Researchers at a web security firm have discovered what they term the latest milestone in the evolving cybercriminal underground: a one-stop-shop for hackers.

Called Golden Cash, the network enables cybercrooks to buy and sell control of compromised computers, as well as trade tools for creating malware and controlling and collecting data from botnets. Also, the platform contains about 100,000 stolen FTP credentials for sale.

The discovery of the Russian-based platform, believed to be run by individuals related to the Russian Business Network (RBN), was noted in the second issue of Finjan's 2009 Cybercrime Intelligence Report. SC Magazine

Full Story :
http://www.scmagazineus.com/Criminal-network-to-trade-botnets-and-malware-uncovered/article/138675/

New Vulnerabilities Tested in SecureScout

- **18415 Buffer Overflow in Print Spooler Vulnerability (MS09-022/961501) (Remote File Checking)**

A remote code execution vulnerability exists in the Windows Print Spooler that could allow a remote, unauthenticated attacker to execute arbitrary code on an affected system. 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.

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

References:

* IDEFENSE: 20090609 Microsoft Windows 2000 Print Spooler Remote Stack Buffer Overflow Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=806
* CONFIRM:
http://support.avaya.com/elmodocs2/security/ASA-2009-217.htm
* MS: MS09-022
http://www.microsoft.com/technet/security/Bulletin/MS09-022.mspx
* BID: 35206
http://www.securityfocus.com/bid/35206
* OSVDB: 54932

http://osvdb.org/54932
* SECTRACK: 1022352
http://www.securitytracker.com/id?1022352
* SECUNIA: 35365
http://secunia.com/advisories/35365
* VUPEN: ADV-2009-1541
http://www.vupen.com/english/advisories/2009/1541

CVE Reference:

CVE-2009-0228 (cve.mitre.org, nvd.nist.gov)

• 18416 Print Spooler Read File Vulnerability (MS09-022/961501) (Remote File Checking)

A local, authenticated information disclosure vulnerability exists in the Windows Printing Service that could allow a user to read or print any file on the system. This action can be taken even if the user does not have administrative access. However, the vulnerability could not be exploited remotely or by anonymous users.

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

References:

* CONFIRM:
http://support.avaya.com/elmodocs2/security/ASA-2009-217.htm
* MS: MS09-022
http://www.microsoft.com/technet/security/Bulletin/MS09-022.mspx
* BID: 35208
http://www.securityfocus.com/bid/35208
* OSVDB: 54933
http://osvdb.org/54933
* SECTRACK: 1022352
http://www.securitytracker.com/id?1022352
* SECUNIA: 35365
http://secunia.com/advisories/35365
* VUPEN: ADV-2009-1541
http://www.vupen.com/english/advisories/2009/1541

CVE Reference:

CVE-2009-0229 (cve.mitre.org, nvd.nist.gov)

• 18417 Print Spooler Load Library Vulnerability (MS09-022/961501) (Remote File Checking)

A remote, authenticated elevation of privilege vulnerability exists in the Windows Print Spooler that could allow an arbitrary dynamic link library (DLL) to be loaded by the Print Spooler. An attacker who successfully exploited this vulnerability could run arbitrary code with elevated privileges. 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:

* CONFIRM:
http://support.avaya.com/elmodocs2/security/ASA-2009-217.htm
* MS: MS09-022
http://www.microsoft.com/technet/security/Bulletin/MS09-022.mspx
* BID: 35209
http://www.securityfocus.com/bid/35209
* OSVDB: 54934
http://osvdb.org/54934
* SECTRACK: 1022352
http://www.securitytracker.com/id?1022352
* SECUNIA: 35365
http://secunia.com/advisories/35365
* VUPEN: ADV-2009-1541
http://www.vupen.com/english/advisories/2009/1541

CVE Reference:

CVE-2009-0230 (cve.mitre.org, nvd.nist.gov)

• 18420 Excel Record Pointer Corruption Vulnerability (CVE-2009-0549) (MS09-021/969462) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Office Excel that could allow remote code execution if a user opens a specially crafted Excel file that includes a malformed record 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: MS09-021
http://www.microsoft.com/technet/security/Bulletin/MS09-021.mspx
* BID: 35215
http://www.securityfocus.com/bid/35215
* OSVDB: 54952
http://osvdb.org/54952
* SECTRACK: 1022351
http://www.securitytracker.com/id?1022351
* VUPEN: ADV-2009-1540
http://www.vupen.com/english/advisories/2009/1540

CVE Reference:

CVE-2009-0549 (cve.mitre.org, nvd.nist.gov)

• 18421 Excel Object Record Corruption Vulnerability (MS09-021/969462) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Office Excel that could allow remote code execution if a user opens a specially crafted Excel file that includes a malformed record 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: MS09-021
http://www.microsoft.com/technet/security/Bulletin/MS09-021.mspx
* BID: 35241
http://www.securityfocus.com/bid/35241
* OSVDB: 54953
http://osvdb.org/54953
* SECTRACK: 1022351
http://www.securitytracker.com/id?1022351
* VUPEN: ADV-2009-1540
http://www.vupen.com/english/advisories/2009/1540

CVE Reference:

CVE-2009-0557 (cve.mitre.org, nvd.nist.gov)

• 18422 Excel Array Indexing Memory Corruption Vulnerability (MS09-021/969462) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Office Excel that could allow remote code execution if a user opens a specially crafted Excel file that includes a malformed record 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:

* BUGTRAQ: 20090609 Secunia Research: Microsoft Excel Record Parsing Array Indexing Vulnerability
http://www.securityfocus.com/archive/1/archive/1/504188/100/0/threaded
* MISC:
http://secunia.com/secunia_research/2009-1/
* MS: MS09-021
http://www.microsoft.com/technet/security/Bulletin/MS09-021.mspx
* BID: 35242
http://www.securityfocus.com/bid/35242
* OSVDB: 54954
http://osvdb.org/54954
* SECTRACK: 1022351
http://www.securitytracker.com/id?1022351

* VUPEN: ADV-2009-1540
http://www.vupen.com/english/advisories/2009/1540

CVE Reference:

CVE-2009-0558 (cve.mitre.org, nvd.nist.gov)

• 18423 Excel String Copy Stack-Based Overrun Vulnerability (MS09-021/969462) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Office Excel that could allow remote code execution if a user opens a specially crafted Excel file that includes a malformed record 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: MS09-021
http://www.microsoft.com/technet/security/Bulletin/MS09-021.mspx
* BID: 35243
http://www.securityfocus.com/bid/35243
* SECTRACK: 1022351
http://www.securitytracker.com/id?1022351
* VUPEN: ADV-2009-1540
http://www.vupen.com/english/advisories/2009/1540

CVE Reference:

CVE-2009-0559 (cve.mitre.org, nvd.nist.gov)

• 18424 Excel Field Sanitization Memory Corruption Vulnerability (MS09-021/969462) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Office Excel that could allow remote code execution if a user opens a specially crafted Excel file that includes a malformed record 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: MS09-021
http://www.microsoft.com/technet/security/Bulletin/MS09-021.mspx
* BID: 35244
http://www.securityfocus.com/bid/35244
* OSVDB: 54956
http://osvdb.org/54956
* SECTRACK: 1022351
http://www.securitytracker.com/id?1022351
* VUPEN: ADV-2009-1540
http://www.vupen.com/english/advisories/2009/1540

CVE Reference:

CVE-2009-0560 (cve.mitre.org, nvd.nist.gov)

• 18425 Excel Record Integer Overflow Vulnerability (MS09-021/969462) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Office Excel that could allow remote code execution if a user opens a specially crafted Excel file that includes a malformed record 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:

* IDEFENSE: 20090609 Microsoft Excel SST Record Integer Overflow Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=805
* BUGTRAQ: 20090609 Secunia Research: Microsoft Excel String Parsing Integer Overflow Vulnerability
http://www.securityfocus.com/archive/1/archive/1/504190/100/0/threaded
* MISC:

http://secunia.com/secunia_research/2009-12/
* MS: MS09-021
http://www.microsoft.com/technet/security/Bulletin/MS09-021.mspx
* BID: 35245
http://www.securityfocus.com/bid/35245
* OSVDB: 54957
http://osvdb.org/54957
* SECTRACK: 1022351
http://www.securitytracker.com/id?1022351
* VUPEN: ADV-2009-1540
http://www.vupen.com/english/advisories/2009/1540

CVE Reference:

CVE-2009-0561 (cve.mitre.org, nvd.nist.gov)

• 18426 Excel Record Pointer Corruption Vulnerability (CVE-2009-1134) (MS09-021/969462) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Office Excel that could allow remote code execution if a user opens a specially crafted Excel file that includes a malformed record 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:

* BUGTRAQ: 20090610 ZDI-09-040: Microsoft Office Excel QSIR Record Pointer Corruption Vulnerability
http://www.securityfocus.com/archive/1/archive/1/504213/100/0/threaded
* MISC:
http://www.zerodayinitiative.com/advisories/ZDI-09-040/
* MS: MS09-021
http://www.microsoft.com/technet/security/Bulletin/MS09-021.mspx
* BID: 35246
http://www.securityfocus.com/bid/35246
* OSVDB: 54958
http://osvdb.org/54958
* SECTRACK: 1022351
http://www.securitytracker.com/id?1022351
* VUPEN: ADV-2009-1540
http://www.vupen.com/english/advisories/2009/1540

CVE Reference:

CVE-2009-1134 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-2064 Microsoft CVSS 2.0 Score = 6.8

Microsoft Internet Explorer 8, and possibly other versions, detects http content in https web pages only when the top-level frame uses https, which allows man-in-the-middle attackers to execute arbitrary web script, in an https site's context, by modifying an http page to include an https iframe that references a script file on an http site, related to "HTTP-Intended-but-HTTPS-Loadable (HPIHSL) pages."

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

References:

MISC: http://research.microsoft.com/pubs/79323/pbp-final-with-update.pdf

MISC: http://research.microsoft.com/apps/pubs/default.aspx?id=79323

CVE Reference: CVE-2009-2064

• CVE-2009-2057 Microsoft CVSS 2.0 Score = 5.8

Microsoft Internet Explorer before 8 uses the HTTP Host header to determine the context of a document provided in a (1) 4xx or (2) 5xx CONNECT response from a proxy server, which allows man-in-the-middle attackers to execute arbitrary web script by modifying this CONNECT response, aka an "SSL tampering" attack.

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

References:

MISC: http://research.microsoft.com/pubs/79323/pbp-final-with-update.pdf

MISC: http://research.microsoft.com/apps/pubs/default.aspx?id=79323

CVE Reference: CVE-2009-2057

- **CVE-2009-2069 Microsoft CVSS 2.0 Score = 5.8**

Microsoft Internet Explorer before 8 displays a cached certificate for a (1) 4xx or (2) 5xx CONNECT response page returned by a proxy server, which allows man-in-the-middle attackers to spoof an arbitrary https site by letting a browser obtain a valid certificate from this site during one request, and then sending the browser a crafted 502 response page upon a subsequent request.

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

References:

MISC: http://research.microsoft.com/pubs/79323/pbp-final-with-update.pdf

MISC: http://research.microsoft.com/apps/pubs/default.aspx?id=79323

CVE Reference: CVE-2009-2069

- **CVE-2008-5515 Apache CVSS 2.0 Score = 5.0**

Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, 6.0.0 through 6.0.18, and possibly earlier versions normalizes the target pathname before filtering the query string when using the RequestDispatcher method, which allows remote attackers to bypass intended access restrictions and conduct directory traversal attacks via .. (dot dot) sequences and the WEB-INF directory in a Request.

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

References:

VUPEN: http://www.vupen.com/english/advisories/2009/1520

BID: http://www.securityfocus.com/bid/35263

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/504202/100/0/threaded

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/504170/100/0/threaded

CONFIRM: http://tomcat.apache.org/security-6.html

CONFIRM: http://tomcat.apache.org/security-5.html

CONFIRM: http://tomcat.apache.org/security-4.html

JVN: http://jvn.jp/en/jp/JVN63832775/index.html

CVE Reference: CVE-2008-5515

- **CVE-2009-1389 Linux CVSS 2.0 Score = 7.8**

Buffer overflow in the RTL8169 NIC driver (drivers/net/r8169.c) in the Linux kernel before 2.6.30 allows remote attackers to cause a denial of service (kernel memory corruption and crash) via a long packet.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=504726

XF: http://xforce.iss.net/xforce/xfdb/51051

MLIST: http://www.openwall.com/lists/oss-security/2009/06/10/1

SECUNIA: http://secunia.com/advisories/35265

MLIST: http://marc.info/?l=linux-netdev&m=123462461713724&w=2

MLIST: http://lkml.org/lkml/2009/6/8/194

CONFIRM: http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=fdd7b4c3302c93f6833e338903ea77245eb510

CVE Reference: CVE-2009-1389

- **CVE-2009-1719 Sun CVSS 2.0 Score = 7.5**

The Aqua Look and Feel for Java implementation in Java 1.5 on Mac OS X 10.5 allows remote attackers to execute arbitrary code via a call to the undocumented apple.laf.CColourUIResource constructor with a crafted value in the first argument, which is dereferenced as a pointer.

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

References:

BID: http://www.securityfocus.com/bid/35401

BID: http://www.securityfocus.com/bid/35381

CONFIRM: http://support.apple.com/kb/HT3632

APPLE: http://lists.apple.com/archives/security-announce/2009/Jun/msg00003.html

MISC: http://www.zerodayinitiative.com/advisories/ZDI-09-043

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/504364/100/0/threaded

CVE Reference: CVE-2009-1719

- **CVE-2009-2058 Apple CVSS 2.0 Score = 6.8**

Apple Safari before 3.2.2 uses the HTTP Host header to determine the context of a document provided in a (1) 4xx or (2) 5xx CONNECT response from a proxy server, which allows man-in-the-middle attackers to execute arbitrary web script by modifying this CONNECT response, aka an "SSL tampering" attack.

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

References:

MISC: http://research.microsoft.com/pubs/79323/pbp-final-with-update.pdf

MISC: http://research.microsoft.com/apps/pubs/default.aspx?id=79323

CVE Reference: CVE-2009-2058

- **CVE-2009-2062 Apple CVSS 2.0 Score = 6.8**

Apple Safari before 3.2.2 processes a 3xx HTTP CONNECT response before a successful SSL handshake, which allows man-in-the-middle attackers to execute arbitrary web script, in an https site's context, by modifying this CONNECT response to specify a 302 redirect to an arbitrary https web site.

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

References:

MISC: http://research.microsoft.com/pubs/79323/pbp-final-with-update.pdf

MISC: http://research.microsoft.com/apps/pubs/default.aspx?id=79323

CVE Reference: CVE-2009-2062

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