netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 18

May 11, 2007

Table of Contents

Product Focus

ASN.1 Vulnerability Scanner – The ASN.1 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 MS04-007 that could allow remote code execution.

This Week in Review

On May 7th 2007, netVigilance released 3 Security Advisories regarding the popular Open Source software "Advanced Guestbook" resulting from Original Security Research done by netVigilance. One of the Vulnerabilities discovered is High Risk with a CVSS Base Score of 8.

This brings the total number of Security advisories released by netVigilance in the last 12 months up to 10.

To see a list of all netVigilance Advisories please go to
http://www.netvigilance.com/advisories

Ipv6 problems. ISS critique of hacking contest. Security holes: Fix or forget? Whitepaper on concerns re web services.

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

❖ Experts scramble to quash IPv6 flaw

'Can be exploited by any greedy Estonian teenager with a $300 Linux machine'
A flawed feature that could amplify denial-of-service attacks on next-generation networks has vendors and engineers rushing to eliminate the potential security issue.

This week, experts sent two drafts to the Internet Engineering Task Force (IETF) - the technical standards-setting body for the internet - proposing different ways of fixing a problem in the way that Internet Protocol version 6 (IPv6) allows the source of network data to determine its path through the network. The drafts recommend that the IPv6 feature should either be eliminated or, at the very least, disabled by default. The specification, known as the Type 0 Routing Header (RH0), allows computers to tell IPv6 routers to send data by a specific route. Originally envisioned as a way to let mobile users to retain a single IP for their devices, the feature has significant security implications. During a presentation at the CanSecWest conference on 18 April, researchers Philippe Biondi and Arnaud Ebalard pointed out that RH0 support allows attackers to amplify denial-of-service attacks on IPv6 infrastructure by a factor of at least 80.

The Register

Full Story :
http://www.theregister.co.uk/2007/05/11/ipv6_flaw_scramble/

❖ ISS slates TippingPoint over hacking contest

IBM's ISS division has torn into rival TippingPoint for sponsoring the hacking contest that led to the disclosure of a QuickTime vul
Such criticism isn't new. Two Gartner analysts, Rich Mogull and Greg Young, made the same point last week in their analysis of April's CanSecWest security conference, which saw $10,000 put up as a prize for managing to hack Apple computers in an open challenge.

The hole that allowed hacking challenger Dino Dai Zovi to win the prize, turned out to be a potentially serious unpatched vulnerability affecting all OS X computers. TippingPoint said that Apple would be informed privately, but others have pointed out this is no guarantee that the exploit information could not have made it into the public domain by other channels.

"The publicity around the contest has exposed thousands of companies to potential compromise through browser attacks, said Kris Lamb of ISS in a statement. "This contest is an excellent example of what can happen when security companies do not have a strict separation of "church and state" between marketing and vulnerability research. nerability in Apple's Safari browser.

techworld

Full Story :
http://www.techworld.com/security/news/index.cfm?newsID=8813&pagtype=samechan

❖ Should vendors close all security holes?

Fix it or forget it? A reader presents an intriguing counterpoint

In last week's column, I argued that vendors should close all known security holes. A reader wrote me with a somewhat interesting argument that I'm still slightly debating, although my overall conclusion stands: Vendors should close all known security holes, whether publicly discussed or not. The idea behind this is that any existing security vulnerability should be closed to strengthen the product and protect consumers. Sounds great, right?

The reader wrote to say that his company often sits on security bugs until they are publicly announced or until at least one customer complaint is made. Before you start disagreeing with this policy, hear out the rest of his argument.

"Our company spends significantly to root out security issues," says the reader. "We train all our programmers in secure coding, and we follow the basic tenets of secure programming design and management. When bugs are reported, we fix them. Any significant security bug that is likely to be high risk or widely used is also immediately fixed. But if we internally find a low- or medium-risk security bug, we often sit on the bug until it is reported publicly. We still research the bug and come up with tentative solutions, but we don't patch the problem."

infoworld

Full Story :
http://www.infoworld.com/article/07/05/11/20OPsecadvise_1.html?source=rss&url=http://www.infoworld.com/article/07/05/11/20OPsecadvise_1.html

❖ Web Services - The Technology and its Security Concerns.

This white paper examines the technology behind Web Services, how the system is made available to the user, and the way connections are made to back-end (and therefore sensitive) data. These different elements come together to make Web Services a portal for users to access data, but also provide different entry points which may be exploited for illegitimate purposes. These security flaws bring about the need for an added security-assessing component in the Acunetix WVS solution. Support for Web Services vulnerability scanning is now provided by a dedicated component which is specifically designed to detect exploitable entry-points in a Web Services system.

tmcnet

Full Story :
http://news.tmcnet.com/news/it/-web-services-technology-its-security-concerns-/2007/05/11/2607724.htm

New Vulnerabilities Tested in SecureScout

- **16507 Microsoft Internet Explorer HTML Objects Memory Corruption Vulnerabilities (MS07-027/931768) (Remote File Checking)**

Several remote code execution vulnerabilities exist in Internet Explorer due to attempts to access uninitialized memory in certain situations. An attacker could exploit these vulnerabilities by constructing a specially crafted Web page. If a user viewed the Web page, these vulnerabilities could allow remote code execution. An attacker who successfully exploited these vulnerabilities could take complete control of an affected system.

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

References:

Original advisory:
MS07-027
http://www.microsoft.com/technet/security/bulletin/ms07-027.mspx

Other references:
* BID:23770
* URL:http://www.securityfocus.com/bid/23770
* FRSIRT:ADV-2007-1712
* URL:http://www.frsirt.com/english/advisories/2007/1712
* SECTRACK:1018019
* URL:http://www.securitytracker.com/id?1018019
* SECUNIA:23769
* URL:http://secunia.com/advisories/23769
* MISC: http://secunia.com/secunia_research/2007-36/advisory/
* BID:23772
* URL:http://www.securityfocus.com/bid/23772

CVE Reference: CVE-2007-0946
CVE Reference: CVE-2007-0947

- **16506 Microsoft Internet Explorer Property Memory Corruption Vulnerability (MS07-027/931768) (Remote File Checking)**

A remote code execution vulnerability exists in the way Internet Explorer handles a property method. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user viewed the Web page. 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:

Original advisory:
MS07-027
http://www.microsoft.com/technet/security/bulletin/ms07-027.mspx

Other references:
BID:23769
URL:http://www.securityfocus.com/bid/23769
FRSIRT:ADV-2007-1712
URL:http://www.frsirt.com/english/advisories/2007/1712
SECTRACK:1018019
URL:http://www.securitytracker.com/id?1018019
SECUNIA:23769
URL:http://secunia.com/advisories/23769

CVE Reference: CVE-2007-0945

❖ 16505 Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability (MS07-027/931768) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer accessing a object when it is not initiated or already deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. If a user viewed the Web page, the vulnerability could allow remote code execution. 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:

Original advisory:
MS07-027
http://www.microsoft.com/technet/security/bulletin/ms07-027.mspx

Other references:
BUGTRAQ:20070508 ZDI-07-027: Microsoft Internet Explorer Table Column Deletion Memory Corruption Vulnerability
#
URL:http://www.securityfocus.com/archive/1/archive/1/467989/100/0/threaded
MISC: http://www.zerodayinitiative.com/advisories/ZDI-07-027.html
BID:23771
URL:http://www.securityfocus.com/bid/23771
FRSIRT:ADV-2007-1712
URL:http://www.frsirt.com/english/advisories/2007/1712
SECTRACK:1018019
URL:http://www.securitytracker.com/id?1018019
SECUNIA:23769
URL:http://secunia.com/advisories/23769

CVE Reference: CVE-2007-0944

❖ 16498 Microsoft Office Drawing Object Vulnerability (MS07-025/934873) (Remote File Checking)

A remote code execution vulnerability exists in the way Microsoft Office handles a specially crafted drawing object. An attacker could exploit this vulnerability when Office parses a file and processes a malformed drawing object. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious Web site. An attacker could exploit the vulnerability by constructing a specially crafted Office file containing a malformed drawing object that could allow remote code execution.

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

References:

Original advisory:
MS07-025
http://www.microsoft.com/technet/security/bulletin/ms07-025.mspx

Other references:
CERT-VN:VU#853184
URL:http://www.kb.cert.org/vuls/id/853184
BID:23826
URL:http://www.securityfocus.com/bid/23826
FRSIRT:ADV-2007-1710
URL:http://www.frsirt.com/english/advisories/2007/1710
SECTRACK:1018014
URL:http://www.securitytracker.com/id?1018014
SECUNIA:25178
URL:http://secunia.com/advisories/25178

CVE Reference: CVE-2007-1747

❖ 16497 Microsoft Word RTF Parsing Vulnerability (MS07-024/934232) (Remote File Checking)

A remote code execution vulnerability exists in the way Microsoft Word parses certain rich text properties within a file. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious Web site. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote code execution.

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

References:

Original advisory:
MS07-024
http://www.microsoft.com/technet/security/bulletin/ms07-024.mspx

Other references:
CERT-VN:VU#555489
URL:http://www.kb.cert.org/vuls/id/555489
BID:23836
URL:http://www.securityfocus.com/bid/23836
FRSIRT:ADV-2007-1709
URL:http://www.frsirt.com/english/advisories/2007/1709
SECTRACK:1018013
URL:http://www.securitytracker.com/id?1018013

CVE Reference: CVE-2007-1202

❖ 16496 Microsoft Word Document Stream Vulnerability (MS07-024/934232) (Remote File Checking)

A remote code execution vulnerability exists in the way Microsoft Word handles a specially crafted Word Document stream. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote code execution.

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

References:

Original advisory:
MS07-024
http://www.microsoft.com/technet/security/bulletin/ms07-024.mspx

Other references:
MISC: http://www.avertlabs.com/research/blog/?p=206
MISC: http://www.microsoft.com/technet/security/advisory/933052.mspx
CERT-VN:VU#332404
URL:http://www.kb.cert.org/vuls/id/332404
BID:22567
URL:http://www.securityfocus.com/bid/22567
FRSIRT:ADV-2007-0607
URL:http://www.frsirt.com/english/advisories/2007/0607
FRSIRT:ADV-2007-1709
URL:http://www.frsirt.com/english/advisories/2007/1709
SECTRACK:1017653
URL:http://www.securitytracker.com/id?1017653
SECUNIA:24122
URL:http://secunia.com/advisories/24122
XF:word-unspecified-string-code-execution(32503)
URL:http://xforce.iss.net/xforce/xfdb/32503

CVE Reference: CVE-2007-0870

❖ 16495 Microsoft Word Array Overflow Vulnerability (MS07-024/934232) (Remote File Checking)

A remote code execution vulnerability exists in the way Microsoft Word handles data within an array. A specially crafted file might be included as an e-mail attachment or hosted on a malicious Web site. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote code execution.

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

References:

Original advisory:
MS07-024
http://www.microsoft.com/technet/security/bulletin/ms07-024.mspx

Other references:
CERT-VN:VU#260777
URL:http://www.kb.cert.org/vuls/id/260777
BID:23804
URL:http://www.securityfocus.com/bid/23804
FRSIRT:ADV-2007-1709
URL:http://www.frsirt.com/english/advisories/2007/1709
SECTRACK:1018013
URL:http://www.securitytracker.com/id?1018013

CVE Reference: CVE-2007-0035

❖ 16494 Microsoft Excel Filter Record Vulnerability (MS07-023/934233) (Remote File Checking)

A remote code execution vulnerability exists in the way Excel handles Excel files with specially crafted filter records. Such a file might be included in an e-mail attachment or hosted on a malicious Web site. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

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

References:

Original advisory:
MS07-023
http://www.microsoft.com/technet/security/bulletin/ms07-023.mspx

Other references:
IDEFENSE:20070508 Microsoft Excel Filter Record Code Execution Vulnerability
URL:http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=527
CERT-VN:VU#253825
URL:http://www.kb.cert.org/vuls/id/253825
BID:23780
URL:http://www.securityfocus.com/bid/23780
FRSIRT:ADV-2007-1708
URL:http://www.frsirt.com/english/advisories/2007/1708
SECTRACK:1018012
URL:http://www.securitytracker.com/id?1018012
SECUNIA:25150
URL:http://secunia.com/advisories/25150

CVE Reference: CVE-2007-1214

❖ 16493 Microsoft Excel Set Font Vulnerability (MS07-023/934233) (Remote File Checking)

A remote code execution vulnerability exists in the way Excel handles Excel files with specially crafted set font values. Such a file might be included in an e-mail attachment or hosted on a malicious Web site. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

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

References:

Original advisory:
MS07-023
http://www.microsoft.com/technet/security/bulletin/ms07-023.mspx

Other references:
BID:23779
URL:http://www.securityfocus.com/bid/23779
FRSIRT:ADV-2007-1708
URL:http://www.frsirt.com/english/advisories/2007/1708
SECTRACK:1018012
URL:http://www.securitytracker.com/id?1018012
SECUNIA:25150
URL:http://secunia.com/advisories/25150

CVE Reference: CVE-2007-1203

❖ 16492 Microsoft Excel BIFF Record Vulnerability (MS07-023/934233) (Remote File Checking)

A remote code execution vulnerability exists in the way Excel handles files with malformed BIFF records. Such a file might be included in an e-mail attachment or hosted on a malicious Web site. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

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

References:

Original advisory:
MS07-023
http://www.microsoft.com/technet/security/bulletin/ms07-023.mspx

Other references:
BUGTRAQ:20070508 ZDI-07-026: Microsoft Excel BIFF File Format Named Graph Record Parsing Stack Overflow Vulnerability
#

URL:http://www.securityfocus.com/archive/1/archive/1/467988/100/0/threaded
MISC: http://www.zerodayinitiative.com/advisories/ZDI-07-026.html
BID:23760
URL:http://www.securityfocus.com/bid/23760
FRSIRT:ADV-2007-1708
URL:http://www.frsirt.com/english/advisories/2007/1708
SECTRACK:1018012
URL:http://www.securitytracker.com/id?1018012
SECUNIA:25150
URL:http://secunia.com/advisories/25150

CVE Reference: CVE-2007-0215

New Vulnerabilities found this Week

Internet Explorer Multiple Vulnerabilities

"Execution of arbitrary code"

Multiple vulnerabilities have been reported in Internet Explorer, which can be exploited by malicious people to compromise a user's system.

1) An error within the instantiation of the chtskdic.dll COM object not intended to be instantiated in Internet Explorer can be exploited to corrupt memory.

2) An error in the "CTableCol::OnPropertyChange()" function when accessing properties of a table column in a named table row after calls to the "deleteCell()" JavaScript method can be exploited to corrupt memory via a specially crafted web page.

3) An error when calling property methods can be exploited to corrupt memory via a specially crafted web page.

4) Errors within the handling of HTML objects can be exploited to corrupt memory via a specially crafted web page.

5) An error in the handling of HTML objects can be exploited to corrupt memory via a specially crafted web page as a CMarkup object is used in certain cases after it has been freed.

6) An error in the media service component (msauth.dll) can be exploited to rewrite arbitrary files via a specially crafted web page.

Successful exploitation of the vulnerabilities allows execution of arbitrary code.

References:
http://www.microsoft.com/technet/security/Bulletin/MS07-027.mspx

Microsoft Office Drawing Object Code Execution Vulnerability

"Execution of arbitrary code"

A vulnerability has been reported in Microsoft Office, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an unspecified error in the parsing of drawing objects and can be exploited via a malicious Office file containing a specially crafted drawing object.

Successful exploitation allows execution of arbitrary code.

References:
http://www.microsoft.com/technet/security/Bulletin/MS07-025.mspx

Cisco IOS FTP Server Multiple Vulnerabilities

"Bypass certain security restrictions; Cause a DoS (Denial of Service)"

Some vulnerabilities have been reported in Cisco IOS, which can be exploited by malicious users and malicious people to bypass certain security restrictions, cause a DoS (Denial of Service), or potentially compromise a vulnerable system.

1) An unspecified error exists in the IOS FTP server when verifying user credentials, which can be exploited to bypass user authentication.

2) An unspecified error exists when transferring files via FTP, which can be exploited to cause a DoS (Denial of Service).

Successful exploitation may allow an attacker to retrieve any file from an affected system (including startup-config), cause IOS to reload, and potentially execute arbitrary code, but requires that the FTP server is enabled, which is not the default setting.

The vulnerabilities are reported in IOS version 11.3, 12.0, 12.1, 12.2, 12.3, and 12.4 containing the FTP server feature.

References:
http://www.cisco.com/en/US/products/products_applied_intelligence_response09186a00808399ea.html
http://www.cisco.com/en/US/products/products_security_advisory09186a00808399d0.shtml

Microsoft Excel Three Code Execution Vulnerabilities

"Execution of arbitrary code"

Three vulnerabilities have been reported in Microsoft Excel, which can be exploited by malicious people to compromise a user's system.

1) A boundary error when handling malformed BIFF records can be exploited to cause a stack-based buffer overflow via a malicious file containing a specially crafted Named Graph record.

2) An error when handling set font values within Excel files can be exploited to corrupt memory via a malicious file containing a specially crafted set font value.

3) An input validation error when handling filter records can be exploited to corrupt memory via a specially crafted file.

Successful exploitation of the vulnerabilities allows execution of arbitrary code.

References:
http://www.microsoft.com/technet/security/Bulletin/MS07-023.mspx

PHP Multiple Vulnerabilities
"Denial of Service"

Several vulnerabilities and weaknesses have been reported in PHP, where some have unknown impacts and others can be exploited by malicious users to manipulate certain data, disclose potentially sensitive information, bypass certain security restrictions, or to cause a DoS (Denial of Service), and potentially by malicious people to compromise a vulnerable system.

1) An input validation error in the "ftp_putcmd()" function can be exploited to inject newline characters.

2) An unspecified error in the "import_request_variables()" can be exploited to overwrite global variables.

3) An unspecified error can remotely be exploited to cause a buffer overflow within in the "make_http_soap_request()" function (PHP 5).

4) An unspecified error can be exploited to cause a buffer overflow within the "user_filter_factory_create()" function (PHP 5).

5) An unspecified error in the bundled libxmlrpc library can remotely be exploited to cause a heap-based buffer overflow and may allow execution of arbitrary code.

6) An input validation error in the "mail()" function allows injection of headers via the "To" and "Subject" parameters.

7) An error in the "mail()" function allows to truncate messages via ASCIIZ bytes.

8) The "safe_mode" and "open_basedir" protection mechanisms can be bypassed via the "zip://" and "bzip://" wrappers.

9) An integer overflow exists in "substr_compare()", which can be exploited to read memory from memory behind PHP variables. The "substr_count" function is reportedly also affected.

10) An error in the "mb_parse_str()" can be exploited to activate "register_globals".

11) An error in the Zend engine related to nested array variables that can be exploited to crash a PHP application.

References:
http://www.php.net/releases/5_2_2.php
http://www.php.net/releases/4_4_7.php

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