netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 27

July 13, 2007

Table of Contents

Product Focus

Task Scheduler Vulnerability Scanner – The Task Scheduler 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 Task Scheduler flaw (MS04-022).

This Week in Review

A look at the threat landscape.Researchers able to download US military data.Help for your server park. The internet is the new operating system.

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

- **Evolving Security Threats Create Challenges**

How Attacks Are Transforming To Target Data
That security threats remain a top concern among data center managers comes as little surprise. What might surprise some, however, is that the threat landscape has been dramatically altered in recent years, such that the average worm proves nearly laughable compared to the more devious threats facing enterprises today.

"In 2007, I expect that we will see the current threat trends continue—namely the move by criminals away from large-scale cyber attacks in favor of more targeted attacks, with a specific focus on stealing confidential information for financial gain via identity theft and even extortion," says Ron O'Brien, senior security analyst with Sophos (www.Processor.com/Sophos1).

Processor

Full Story :
http://www.processor.com/editorial/article.asp?Article=articles/p2928/20p28/20p28.asp&GUID=59AB119B42F44DF7B8702AF8BF89CFB2

❖ Sensitive U.S. military files accessible on the Net

A lack of adequate protections on file servers run by government agencies and military subcontractors allowed reporters for the Associated Press to download sensitive military and technical files from computers that should not have allowed public access, the news service reported on Thursday.

The files included information that could have allowed hackers access to Department of Defense computer systems, maps of military facilities in Iraq, descriptions of the security features at some of the facilities, and plans for infrastructure improvement at bases in the Middle East, the AP reported. The files were hosted on anonymous FTP (File Transfer Protocol) servers with no password protection or, in one case, with a password that was included in another file on the server.

Securityfocus

Full Story :
http://www.securityfocus.com/brief/546?ref=rss

❖ Best Practices: Server Operating System Security

Security managers are at their wits' ends trying to keep their servers secure from the deluge of new vulnerabilities across all operating systems. Why? Because as systems grow more complex, it becomes more difficult to maintain proper access controls and mitigate new vulnerabilities. To uncover server security best practices, Forrester spoke with 137 leading firms handling large numbers of servers. Our research uncovered best practices in three areas: server patching, server hygiene, and access control. Sound obvious? Perhaps, but our research revealed that very few security managers manage to deploy most of these best practices consistently and effectively.

forrester

Full Story :
http://www.forrester.com/Research/Document/Excerpt/0,7211,40478,00.html

❖ Going from killer app to major Web platform

They all started out as applications that evolved into Web platforms, enabling developers

to create more compatible programs and companies to build businesses off the platform ecosystem. This is the wave of the future, company executives said in a panel on Thursday at Fortune magazine's first iMeme: Thinkers of Tech conference, an event striving so hard for chicness that it opened with a lesson on how to operate the Herman Miller Aeron chairs filling the room at the Ritz-Carlton hotel in San Francisco.

"The Internet is the new operating system. The killer apps of the Internet are becoming platforms that are creating communities of innovation," said Marc Benioff, chief executive of customer-relationship management specialist Salesforce.com. "This is a whole new chapter in our industry."

Cnet news

Full Story :
http://news.com.com/Going+from+killer+app+to+major+Web+platform/2100-1032_3-6196341.html?tag=newsmap

New Vulnerabilities Tested in SecureScout

- **16556 Microsoft IIS Memory Request Vulnerability (MS07-041/939373) (Remote File Checking)**

There is a remote code execution vulnerability in Internet Information Services (IIS) 5.1 on Windows XP Professional Service Pack 2 that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system. An attacker could exploit the vulnerability by sending specially crafted URL requests to a Web page hosted by Internet Information Services.

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

References:

Original advisory:
* MS:MS07-041
http://www.microsoft.com/technet/security/Bulletin/ms07-041.mspx

CVE Reference: CVE-2005-4360

- **16555 Microsoft Publisher Invalid Memory Reference Vulnerability (MS07-037/936548) (Remote File Checking)**

A remote code execution vulnerability exists in the way Publisher does not adequately clear out memory resources when writing application data from disk to memory. An attacker could exploit the vulnerability by constructing a specially crafted Publisher (.pub) page. When a user views the .pub 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:
* MS:MS07-037
http://www.microsoft.com/technet/security/Bulletin/ms07-037.mspx

CVE Reference: CVE-2007-1754

❖ 16554 Microsoft .NET JIT Compiler Vulnerability (MS07-040/931212) (Remote File Checking)

A remote code execution vulnerability exists in .NET Framework Just In Time Compiler that could allow an attacker who successfully exploited this vulnerability to make changes to the system with the permissions of the logged-on user. If a user is logged on with administrative user rights, an attacker could take complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

Original advisory:
* MS:MS07-040
http://www.microsoft.com/technet/security/Bulletin/ms07-040.mspx

CVE Reference: CVE-2007-0043

❖ 16553 Microsoft ASP.NET Null Byte Termination Vulnerability (MS07-040/931212) (Remote File Checking)

An information disclosure vulnerability exists in .NET Framework that could allow an attacker who successfully exploited this vulnerability to bypass the security features of an ASP.NET Web site to download the contents of any Web page.

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

References:

Original advisory:
* MS:MS07-040
http://www.microsoft.com/technet/security/Bulletin/ms07-040.mspx

CVE Reference: CVE-2007-0042

❖ 16552 Microsoft .NET PE Loader Vulnerability (MS07-040/931212) (Remote File Checking)

A remote code execution vulnerability exists in .NET Framework that could allow an attacker who successfully exploited this vulnerability to make changes to the system with the permissions of the logged-on user. If a user is logged in with administrative user rights, an attacker could take complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

Original advisory:
* MS:MS07-040
http://www.microsoft.com/technet/security/Bulletin/ms07-040.mspx

CVE Reference: CVE-2007-0041

❖ 16551 Microsoft Windows Active Directory Denial of Service Vulnerability (MS07-039/926122) (Remote File Checking)

A denial of service vulnerability exists in the way that Microsoft Active Directory validates a client-sent LDAP request. An attacker could exploit the vulnerability by sending a specially crafted LDAP request to a server running Active Directory. An attacker who successfully exploited this vulnerability could cause the server to temporarily stop responding.

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

References:

Original advisory:
* MS:MS07-039
http://www.microsoft.com/technet/security/Bulletin/ms07-039.mspx

CVE Reference: CVE-2007-3028

❖ 16550 Microsoft Windows Active Directory Remote Code Execution Vulnerability (MS07-039/926122) (Remote File Checking)

A remote code execution vulnerability exists in the way that Active Directory validates a LDAP request. 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:
* MS:MS07-039
http://www.microsoft.com/technet/security/Bulletin/ms07-039.mspx

CVE Reference: CVE-2007-0040

❖ 16549 Microsoft Excel Workbook Memory Corruption Vulnerability (MS07-036/936542) (Remote File Checking)

A remote code execution vulnerability exists in the way Excel handles malformed Excel files. An attacker could exploit the vulnerability by sending a malformed file which could be included as an e-mail attachment, or hosted on a malicious or compromised Web site.

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

References:

Original advisory:
* MS:MS07-036
http://www.microsoft.com/technet/security/Bulletin/ms07-036.mspx

CVE Reference: CVE-2007-3030

❖ 16548 Microsoft Excel Worksheet Memory Corruption Vulnerability (MS07-036/936542) (Remote File Checking)

A remote code execution vulnerability exists in the way Excel handles malformed Excel files. An attacker could exploit the vulnerability by sending a malformed file which could be included as an e-mail attachment, or hosted on a malicious or compromised Web site.

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

References:

Original advisory:
* MS:MS07-036
http://www.microsoft.com/technet/security/Bulletin/ms07-036.mspx

CVE Reference: CVE-2007-3029

❖ 16547 Microsoft Excel Calculation Error Vulnerability (MS07-036/936542) (Remote File Checking)

A remote code execution vulnerability exists in the way Excel handles malformed Excel files. An attacker could exploit the vulnerability by sending a malformed file

which could be included as an e-mail attachment, or hosted on a malicious or compromised Web site.

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

References:

Original advisory:
* MS:MS07-036
http://www.microsoft.com/technet/security/Bulletin/ms07-036.mspx

CVE Reference: CVE-2007-1756

New Vulnerabilities found this Week

Apple QuickTime Multiple Vulnerabilities
"Execution of arbitrary code"

Some vulnerabilities have been reported in Apple QuickTime, which can be exploited by malicious people to compromise a user's system.

1) An unspecified error exists in the processing of H.264 movies. This can be exploited to cause memory corruption and may allow execution of arbitrary code when a user accesses a specially crafted H.264 movie.

2) An unspecified error exists in the processing of movie files. This can be exploited to cause memory corruption and may allow execution of arbitrary code when a user accesses a specially crafted movie file.

3) An integer overflow error exists in the handling of .m4v files and can be exploited to execute arbitrary code when a user accesses a specially crafted .m4v file.

4) An integer overflow error exists in the handling of the "author" and "title" fields when parsing SMIL files. This can be exploited to cause a heap-based buffer overflow and may allow execution of arbitrary code when a user opens a specially crafted SMIL file.

5) A design error exists in QuickTime for Java, which can be exploited to disable security checks and execute arbitrary code when a user visits a web site containing a specially crafted Java applet.

6) A design error exists in QuickTime for Java, which can be exploited to bypass security checks and read and write to process memory. This can lead to execution of arbitrary code when a user visits a web site containing a specially crafted Java applet.

7) A design error exists in QuickTime for Java due to JDirect exposing interfaces that may allow loading arbitrary libraries and freeing arbitrary memory. This can be exploited to execute arbitrary code when a user visits a web site containing a specially crafted Java applet.

8) A design error exists in QuickTime for Java, which can be exploited to capture the user's screen content when a user visits a web site containing a specially crafted Java

applet.

The vulnerabilities are reported in versions prior to 7.2.

References:
http://docs.info.apple.com/article.html?artnum=305947
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=556

Adobe Flash Player Multiple Vulnerabilities

"Gain knowledge of sensitive information"

Some vulnerabilities have been reported in Adobe Flash Player, which can be exploited by malicious people to gain knowledge of sensitive information or compromise a user's system.

1) An input validation error can be exploited to execute arbitrary code when a user e.g. visits a malicious website.

The vulnerability affects versions 9.0.45.0 and prior.

2) An error within the interaction of Flash Player and certain browsers can be exploited to leak key presses to a Flash Player applet.

The vulnerability affects versions 7.0.69.0 and prior on Linux and Solaris. It does not affect Flash Player 9.

A bug has also been reported in the validation of the HTTP Referer in versions 8.0.34.0 and prior, which may aid in e.g. CSRF (Cross-Site Request Forgery) attacks.

References:
http://www.adobe.com/support/security/bulletins/apsb07-12.html

AVG Antivirus AVG7CORE.SYS IOCTL Handler Privilege Escalation

"Gain escalated privileges"

Jonathan Lindsay has reported a vulnerability in AVG Antivirus, which potentially can be exploited by malicious, local users to gain escalated privileges.

An input validation error within the 0x5348E004 IOCTL handler of the AVG7CORE.SYS device driver and insecure permissions on the device interface can be exploited e.g. to access the affected IOCTL handler and overwrite arbitrary kernel memory.

The vulnerability is reported in AVG7CORE.SYS version 7.5.0.444 included in AVG Free 7.5.446 and AVG Antivirus 7.5.448.

Symantec Products Real-Time Scanner Notification Window Privilege Escalation

"Gain escalated privileges"

A vulnerability has been reported in some Symantec products, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to an error in the Real-Time scanner (RTVScan) component when displaying a notification window containing information on threats found on a system. This can be exploited to execute arbitrary code with SYSTEM privileges.

The vulnerability is reported in the following products and versions:
* Symantec AntiVirus Corporate Edition versions 9.0, 10.0 and 10.1
* Symantec Client Security versions 2.0, 3.0, and 2.1

References:
http://securityresponse.symantec.com/avcenter/security/Content/2007.07.11c.html

Microsoft Patch Tuesday July 2007
"Denial of service; Code execution; Information disclosure"

This past Tuesday, Microsoft released patches for 6 products.

Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (936542)
Vulnerability in Windows Active Directory Could Allow Remote Code Execution (926122)
Vulnerabilities in .NET Framework Could Allow Remote Code Execution (931212)
Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution (936548)
Vulnerability in Microsoft Internet Information Services Could Allow Remote Code Execution (939373)
Vulnerability in Windows Vista Firewall Could Allow Information Disclosure (935807)

References:
http://www.microsoft.com/technet/security/bulletin/ms07-jul.mspx
http://www.microsoft.com/technet/security/Bulletin/ms07-036.mspx
http://www.microsoft.com/technet/security/Bulletin/ms07-037.mspx
http://www.microsoft.com/technet/security/Bulletin/ms07-038.mspx
http://www.microsoft.com/technet/security/Bulletin/ms07-039.mspx
http://www.microsoft.com/technet/security/Bulletin/ms07-040.mspx
http://www.microsoft.com/technet/security/Bulletin/ms07-041.mspx
http://descriptions.securescout.com/tc/16547
http://descriptions.securescout.com/tc/16548
http://descriptions.securescout.com/tc/16549
http://descriptions.securescout.com/tc/16550
http://descriptions.securescout.com/tc/16551
http://descriptions.securescout.com/tc/16552
http://descriptions.securescout.com/tc/16553
http://descriptions.securescout.com/tc/16554
http://descriptions.securescout.com/tc/16555
http://descriptions.securescout.com/tc/16556

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