netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 46

November 17, 2006

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

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

UK incorporates tougher penalties for hacking. Survey on financial services' security. Risks when sharing data with third party. Experts call for stronger data security .

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

- **Denial of service becomes criminal offence**

Tougher penalties for hackers and internet offenders have now been incorporated into the UK's Computer Misuse Act.

Amendments to the 1990 law now make it an offence to launch a denial of service (DoS) attack in the UK which will be punishable by up to 10 years in prison.

These are attacks in which a web or email server is deliberately flooded with information

to the point of collapse.

There has been ongoing concern that the CMA, which was written before the days when the public and companies had general access to the World Wide Web, was outdated. For example DoS attacks were not covered.

Law firm Pinsent Masons online advice and guidance service Out-Law pointed out that when a court cleared teenager David Lennon in November 2005 on charges of sending five million emails to his former employer – because the judge decided that no offence had been committed under the Act – the need for amendment seemed obvious.

Computeractive

Full Story :
http://www.computeractive.co.uk/computeractive/news/2168599/denial-service-becomes-criminal

- **Financial Services Among Top Companies Making Strong Case for Security Programs**

The Conference Board (New York) recently released a study that illustrated companies most attuned to security issues are those with the most exposure to a broad range of security risks—including organizations in critical infrastructure industries, large corporations, multinationals with global operations and publicly-traded companies.

The survey, "Navigating Risk: The Business Case for Security," was sponsored by the Department of Homeland Security and was designed to gauge the role and influence of security managers among general senior executives. What it found was that the most supportive executives were not necessarily the most influential, and the most influential managers were not necessarily the most supportive.

The Conference Board surveyed 213 senior corporate executives in a variety of industries, 30 of whom were from financial services, one of the largest sample groups represented. "Financial services is generally seen as one of the pace-setter industries in security," comments Thomas Cavanaugh, senior research associate in global corporate citizenship at The Conference Board and author of the report.

Wallstreet&Technology

Full Story :
http://www.wstonline.com/news/operations/showArticle.jhtml;jsessionid=LYIZXJ0GRKFPAQSNDLRSKHSCJUNN2JVN?articleID=194400553

- **Firms must face third-party security risks**

Over half of organisations are failing to manage the risks of sharing data with third parties, although many are now investing in securing the capture and storage of sensitive data, according to a new global survey by consultancy Ernst & Young.

The firm's Global Information Security Survey of 1,200 public and private sector organisations in nearly 50 countries found that more than three-quarters cited privacy

and data protection as a significant issue; with 52 percent addressing privacy and data protection with formal procedures.

"It's been an issue for years but it has been done in an ad-hoc way through point solutions," explained the firm's UK head of Technology and Security Risk Services, Richard Brown. "But now consumers are being more savvy in that area, and organisations are getting on top of segregation of duties and securing data. "

ITWeek

Full Story :
http://www.itweek.co.uk/itweek/news/2168827/firms-face-third-party-security

- **Experts Challenge Industry to Improve Data Security by Matching Cryptographic Schemes**

Participants in third annual Certicom ECC Conference discuss security issues, solutions and evolving security standards

MISSISSAUGA, ON, Nov. 16 /PRNewswire-FirstCall/ - Data security may be a priority for most executives but the cryptographic schemes many are using have fundamental weaknesses. This was one of the recurring issues raised at the Certicom ECC Conference, which concludes today in Toronto, Ontario. For three days, some of the finest minds in cryptography and the security industry, representing Canada, the United States, Europe and Asia, discussed security issues, real-world applications of cryptography and evolving security standards.

The participants agreed that while most security executives use the Advanced Encryption Standard (AES) with 128 bits of security, for optimal security they also need to ensure that the corresponding public-key scheme for key management and authentication matches the AES in strength. Cryptography is a basic component used in security mechanisms to protect data in consumer electronics, wireless devices and semiconductors as well as other applications used in financial services and government markets.

PR Newswire

Full Story :
http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=ind_focus.story&STORY=/www/story/11-16-2006/0004476184&EDATE=THU+Nov+16+2006,+11:41+AM

New Vulnerabilities Tested in SecureScout

- **12144 SSL Server invalid CN in Certificate Vulnerability**

SSL is a network layer that allows privacy in communications. Servers supporting SSL should use valid certificates.

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

References:

About the risk of using invalid certificates:
http://www.rsasecurity.com/products/keon/datasheets/KWS_DS_0702.pdf

CVE Reference:

❖ 12145 SSL Server untrusted Root certificate Vulnerability

SSL is a network layer that allows privacy in communications. Servers supporting SSL should use valid certificates.

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

References:

About the risk of using invalid certificates:
http://www.rsasecurity.com/products/keon/datasheets/KWS_DS_0702.pdf

CVE Reference:

❖ 12146 SSL Server Revoked Certificate or Signature Vulnerability

SSL is a network layer that allows privacy in communications. Servers supporting SSL should use valid certificates.

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

References:

About the risk of using invalid certificates:
http://www.rsasecurity.com/products/keon/datasheets/KWS_DS_0702.pdf

CVE Reference:

❖ 12147 SSL Server validity periods of the certification chain not nesting correctly Vulnerability

SSL is a network layer that allows privacy in communications. Servers supporting SSL should use valid certificates.

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

References:

About the risk of using invalid certificates:
http://www.rsasecurity.com/products/keon/datasheets/KWS_DS_0702.pdf

CVE Reference:

❖ 13475 Oracle Database Server - DDL component unspecified

Vulnerability (Alert 68/aug-04/DB17)

An unspecified vulnerability exists in Oracle Database Server DDL component.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf

Other references:
iDEFENSE:
http://www.idefense.com/application/poi/display?id=135&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=136&type=vulnerabilities

Red Database Security:
http://www.red-database-security.com/advisory/advisory_20040903_1.html
http://www.red-database-security.com/advisory/advisory_20040903_2.html
http://www.red-database-security.com/advisory/advisory_20040903_3.html

Application Security:
http://www.appsecinc.com/resources/alerts/oracle/2004-0001/

Integrigy:
http://www.integrigy.com/alerts/OraAlert68OraAppsImpact.htm

Pentest Limited:
http://www.pentest.co.uk/documents/ptl-2004-04.html

US-CERT VU#170830:
http://www.kb.cert.org/vuls/id/170830

US-CERT VU#435974:
http://www.kb.cert.org/vuls/id/435974

US-CERT VU#316206:
http://www.kb.cert.org/vuls/id/316206

BID:11099
http://www.securityfocus.com/bid/11099

BID:11100
http://www.securityfocus.com/bid/11100

BID:10871
http://www.securityfocus.com/bid/10871

Secunia:
http://secunia.com/advisories/12409/

Product Homepage:
http://www.oracle.com/

CVE Reference: CVE-2004-0637
CAN-2004-0638
CAN-2004-1338
CAN-2004-1339
CAN-2004-1362
CAN-2004-1363
CAN-2004-1364
CAN-2004-1366
CAN-2004-1367
CAN-2004-1368
CAN-2004-1369
CAN-2004-1370

CAN-2004-1371

❖ 16360 Vulnerabilities in Client Service for NetWare Could Allow Remote Code Execution (MS06-066/923980) (Remote File Checking)

There is a remote code execution vulnerability in Client Service for NetWare (CSNW) that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

A denial of service vulnerability exists in Client Service for NetWare (CSNW) that could allow an attacker to send a specially crafted network message to an affected system running the Client Service for NetWare service. An attacker could cause the system to stop responding.

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

References:

Original advisory:
MS06-066
http://www.microsoft.com/technet/security/bulletin/ms06-066.mspx

Other references:
* FRSIRT:ADV-2006-4504
* URL:http://www.frsirt.com/english/advisories/2006/4504
* SECUNIA:22866
* URL:http://secunia.com/advisories/22866
* XF:ms-csnw-bo(29952)
* URL:http://xforce.iss.net/xforce/xfdb/29952

CVE Reference: CVE-2006-4688
CVE-2006-4689

❖ 16361 Cumulative Security Update for Internet Explorer (MS06-067/922760) (Remote File Checking)

Remote code execution vulnerabilities exist in DirectAnimation ActiveX controls that could be exploited if the ActiveX controls are passed unexpected data. An attacker could exploit these vulnerabilities by constructing a specially crafted Web page that could potentially allow remote code execution if a user visited the specially crafted Web page. An attacker who successfully exploited these vulnerabilities could take complete control of an affected system.

A remote code execution vulnerability exists in the way Internet Explorer interprets HTML with certain layout combinations. 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:
MS06-067
http://www.microsoft.com/technet/security/bulletin/ms06-067.mspx

Other references:
* BUGTRAQ:20060913 [0day] daxctle2.c - Internet Explorer COM Object Heap Overflow Download Exec Exploit
* URL:http://www.securityfocus.com/archive/1/archive/1/445898/100/0/threaded
* BUGTRAQ:20060915 Fwd: IE ActiveX 0day?
* URL:http://www.securityfocus.com/archive/1/archive/1/446065/100/0/threaded
* BUGTRAQ:20060915 RE: IE ActiveX 0day?
* URL:http://www.securityfocus.com/archive/1/archive/1/446084/100/0/threaded
* BUGTRAQ:20060915 Re: Fwd: IE ActiveX 0day?
* URL:http://www.securityfocus.com/archive/1/archive/1/446085/100/0/threaded
* BUGTRAQ:20060918 Re: IE ActiveX 0day?
* URL:http://www.securityfocus.com/archive/1/archive/1/446246/100/0/threaded
* MISC: http://www.milw0rm.com/exploits/2358
* MISC: http://www.xsec.org/index.php?module=releases&act=view&type=2&id=20
* CONFIRM: http://www.microsoft.com/technet/security/advisory/925444.mspx
* CERT-VN:VU#377369
* URL:http://www.kb.cert.org/vuls/id/377369
* BID:20047
* URL:http://www.securityfocus.com/bid/20047
* FRSIRT:ADV-2006-3593
* URL:http://www.frsirt.com/english/advisories/2006/3593
* OSVDB:28842
* URL:http://www.osvdb.org/28842
* SECTRACK:1016854
* URL:http://securitytracker.com/id?1016854
* SECUNIA:21910
* URL:http://secunia.com/advisories/21910
* XF:ie-directanimation-code-execution(28942)
* URL:http://xforce.iss.net/xforce/xfdb/28942
* BUGTRAQ:20060827 [XSec-06-10]: Internet Explorer (daxctle.ocx) Heap Overflow Vulnerability
* URL:http://www.securityfocus.com/archive/1/archive/1/444504/100/0/threaded
* MISC: http://www.xsec.org/index.php?module=releases&act=view&type=1&id=19
* BID:19738
* URL:http://www.securityfocus.com/bid/19738
* OSVDB:28841
* URL:http://www.osvdb.org/28841
* SECTRACK:1016764
* URL:http://securitytracker.com/id?1016764
* XF:ie-daxctle-dos(28608)
* URL:http://xforce.iss.net/xforce/xfdb/28608
* MISC: http://www.zerodayinitiative.com/advisories/ZDI-06-041.html
* FRSIRT:ADV-2006-4505
* URL:http://www.frsirt.com/english/advisories/2006/4505

CVE Reference: CVE-2006-4777
CVE-2006-4446

CVE-2006-4687

❖ 16362 Vulnerability in Microsoft Agent Could Allow Remote Code Execution (MS06-068/920213) (Remote File Checking)

There is a remote code execution vulnerability in the way that Microsoft Agent handles specially crafted .ACF files. 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:
MS06-068
http://www.microsoft.com/technet/security/bulletin/ms06-068.mspx

Other references:
* FRSIRT:ADV-2006-4506
* URL:http://www.frsirt.com/english/advisories/2006/4506
* SECUNIA:22878
* URL:http://secunia.com/advisories/22878
* XF:ms-agent-acf-bo(29945)
* URL:http://xforce.iss.net/xforce/xfdb/29945

CVE Reference: CVE-2006-3445

❖ 16364 Vulnerability in Workstation Service Could Allow Remote Code Execution (MS06-070/924270) (Remote File Checking)

A remote code execution vulnerability exists in the Workstation service that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

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

References:

Original advisory:
MS06-070
http://www.microsoft.com/technet/security/bulletin/ms06-070.mspx

Other references:
* FRSIRT:ADV-2006-4508
* URL:http://www.frsirt.com/english/advisories/2006/4508
* SECUNIA:22883
* URL:http://secunia.com/advisories/22883
* XF:win-workstation-service-bo(29948)
* URL:http://xforce.iss.net/xforce/xfdb/29948

CVE Reference: CVE-2006-4691

❖ **16365 Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (MS06-071/928088) (Remote File Checking)**

A vulnerability exists in the XMLHTTP ActiveX control within Microsoft XML Core Services that could allow for remote code execution. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user visited that page or clicked a link in an e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, user interaction is required to exploit this vulnerability.

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

References:

Original advisory:
MS06-071
http://www.microsoft.com/technet/security/bulletin/ms06-071.mspx

Other references:
* MISC: http://xforce.iss.net/xforce/alerts/id/239
* MISC: http://blogs.securiteam.com/?p=717
* CONFIRM: http://www.microsoft.com/technet/security/advisory/927892.mspx
* CERT-VN:VU#585137
* URL:http://www.kb.cert.org/vuls/id/585137
* BID:20915
* URL:http://www.securityfocus.com/bid/20915
* FRSIRT:ADV-2006-4334
* URL:http://www.frsirt.com/english/advisories/2006/4334
* SECTRACK:1017157
* URL:http://securitytracker.com/id?1017157
* SECUNIA:22687
* URL:http://secunia.com/advisories/22687
* XF:ie-xml-http-request-handling(30004)
* URL:http://xforce.iss.net/xforce/xfdb/30004

CVE Reference: CVE-2006-5745

New Vulnerabilities found this Week

WinZip FileView ActiveX Control Multiple Vulnerabilities

"Execute arbitrary code"

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

1) Several unspecified insecure methods exist in the FileView ActiveX control (WZFILEVIEW.FileViewCtrl.61). This can be exploited to execute arbitrary code when a

user e.g. visits a malicious website.

2) A boundary error in the FileView ActiveX control within the handling of the "filepattern" property can be exploited to cause a buffer overflow.

The vulnerabilities are reported in WinZip 10.0 versions prior to Build 7245.

References:
http://www.winzip.com/wz7245.htm
http://www.zerodayinitiative.com/advisories/ZDI-06-040.html
http://www.kb.cert.org/vuls/id/225217
http://www.kb.cert.org/vuls/id/512804

Adobe Flash Player CRLF Injection Vulnerabilities

"Make it easier to perform CSRF"

Rapid7 has reported some vulnerabilities in Adobe Flash Player, which can be exploited by malicious people to bypass certain restrictions.

Input passed to the "XML.addRequestHeader()" ActionScript function and the "XML.contentType" attribute is not properly sanitized before being used. This can be exploited to bypass certain restrictions via CRLF character sequences and inject arbitrary HTTP headers in a request.

Successful exploitation may e.g. make it easier to perform CSRF (Cross-Site Request Forgery) attacks.

The vulnerabilities are reported in version 9.0.16 for Windows and 7.0.63 for Linux. According to the vendor, all current versions from 7.x through 9.x are affected.

References:
http://www.adobe.com/support/security/bulletins/apsb06-18.html
http://www.rapid7.com/advisories/R7-0026.jsp

Panda ActiveScan Multiple Vulnerabilities

"Denial of Service; disclose system information"

Secunia Research has discovered two vulnerabilities and a weakness in Panda ActiveScan, which can be exploited by malicious people to disclose system information, cause a DoS (Denial of Service), and compromise a user's system.

1) The "Reinicializar()" method in the "ActiveScan.1" ActiveX control allows rebooting the system when invoked. This can be exploited by e.g. a malicious website to reboot a user's system without any user confirmation.

2) The "ObtenerTamano()" method in the "PAVPZ.SOS.1" ActiveX control returns the file size of a given local filename. This can be exploited by e.g. a malicious website to determine the presence of local files and the corresponding file sizes.

3) The "Analizar()" method in the "ActiveScan.1" ActiveX control is not thread safe. This can be exploited by e.g. a malicious website via a race condition to corrupt memory and execute arbitrary code.

The vulnerabilities are confirmed in version 5.53.00. Other versions may also be affected.

References:
http://secunia.com/secunia_research/2006-64/

Sun Solaris libXfont Integer Overflow Vulnerability
"Denial of Service"

Sun has acknowledged a vulnerability in Sun Solaris, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102714-1
http://secunia.com/advisories/20100/

VMware ESX Server Multiple Vulnerabilities
"Disclose potentially sensitive information; Denial of Service"

Some vulnerabilities, security issues, and a weakness have been reported in VMware ESX Server, which can be exploited by malicious, local users to bypass certain security restrictions and disclose potentially sensitive information, or by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

References:
http://www.vmware.com/download/esx/esx-253-200610-patch.html
http://www.vmware.com/download/esx/esx-254-200610-patch.html
http://www.vmware.com/download/esx/esx-213-200610-patch.html
http://www.vmware.com/download/esx/esx-202-200610-patch.html

Microsoft Patch Tuesday
"Remote code execution; Denial of Service"

Microsoft released the following Security related bulletins, fixing several remote code execution and Denial of Service vulnerabilities.

* Vulnerabilities in Client Service for NetWare Could Allow Remote Code Execution (MS06-066/923980)
* Cumulative Security Update for Internet Explorer (MS06-067/922760)
* Vulnerability in Microsoft Agent Could Allow Remote Code Execution (MS06-068/920213)
* Vulnerability in Workstation Service Could Allow Remote Code Execution (MS06-070/924270)
* Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (MS06-071/928088)
* Vulnerabilities in Macromedia Flash Player from Adobe Could Allow Remote Code Execution (MS06-069/923789) (Remote File Checking)

References:
http://www.microsoft.com/technet/security/bulletin/ms06-066.mspx
http://www.microsoft.com/technet/security/bulletin/ms06-067.mspx
http://www.microsoft.com/technet/security/bulletin/ms06-068.mspx

http://www.microsoft.com/technet/security/bulletin/ms06-069.mspx
http://www.microsoft.com/technet/security/bulletin/ms06-070.mspx
http://www.microsoft.com/technet/security/bulletin/ms06-071.mspx
http://descriptions.securescout.com/tc/16360
http://descriptions.securescout.com/tc/16361
http://descriptions.securescout.com/tc/16362
http://descriptions.securescout.com/tc/16364
http://descriptions.securescout.com/tc/16365

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