netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 50

December 21, 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

Jesper Jurcenoks of netVigilance speaks about va. Risk assessment - how to. A little new year's dream. Some good advice.

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

- **NetVigilance CTO Jesper Jurcenoks Speaks**

Jesper Jurcenoks, technical leader of NetVigilance.com, says if a device has a TCP/IP address, his software can test it for vulnerabilities. With customers ranging from 10 devices to over 100,000, Jurcenoks has seen plenty and shares his considerable expertise in network vulnerability assessment in this video interview.

podtech

Full Story :
http://www.podtech.net/home/4758/netvigilance-cto-jesper-jurcenoks-speaks

❖ Know Which Risks Matter

CIOs are frequently asked, “What are our IT risks?” Unfortunately, this question is too generic, since there are multiple kinds of risk. Before starting any risk assessment, IT needs to understand both the concern prompting the request and which risks need to be assessed. Moreover, everyone needs to understand that nearly all risks that affect an IT organization affect the entire business.

Risks fall into four categories that require different mitigation tools:

Business operations risk. An assessment determines the risks involved in addressing or ignoring a particular competitive threat. Analyzing competitive threats helps the company decide whether to invest the resources necessary to combat the threat.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=308347&taxonomyId=17&intsrc=kc_feat

❖ Dreaming the impossible dream for 2008: A patch-free year

So here we are at the end of yet another year. It's always a whole lot easier to look back than to look forward, but if there's one thing that stays with us from year to year, it's security, or, rather the lack of it in many cases.

A year ago at this time, I was just returning from Microsoft's Redmond campus, after getting an immersion treatment into Windows Vista security. Zillions of dollars were spent completely re-architecting the way Windows handled security. Dozens of experts from around the world were flown to Redmond for conferences over Vista's five-year gestation period with the express mission of breaking into the code and finding every last possible weakness.

IT World

Full Story :
http://security.itworld.com/4940/patch-free-systems-integrators-nlssolutions-071219/page_1.html

❖ Be Careful What You Write For It Lives Forever

I was as bad as Bart Simpson. Like the little spiky yellow-haired terror of TV, when I was 10 years old I made more than my fair share of crank phone calls. Fortunately, the chuckles my friend Mike and I got from asking some poor old lady if her washing machine was running ("well, lady, you better go catch it!") or if her pipe-smoking husband had Sir

Walter Raleigh in the can ("you better let him out!") were mere moments in time, here one instant and gone forever the next. Not so today with e-mail, documents saved to a server, and most recently, the blogosphere.

IT World

Full Story :
http://security.itworld.com/5009/nlssi-email-security-privacy071206/page_1.html

New Vulnerabilities Tested in SecureScout

- **16677 Oracle Application Server - Oracle Portal component unspecified Vulnerability (oct-2007/AS11)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Portal component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html
* CERT: TA07-290A
http://www.us-cert.gov/cas/techalerts/TA07-290A.html
* FRSIRT: ADV-2007-3524
http://www.frsirt.com/english/advisories/2007/3524
* SECTRACK: 1018823
http://www.securitytracker.com/id?1018823
* SECUNIA: 27251
http://secunia.com/advisories/27251

CVE Reference: CVE-2007-5526

- **16676 Oracle Application Server - Oracle Single Sign-On component unspecified Vulnerability (oct-2007/AS10)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Single Sign-On component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html
* CERT: TA07-290A
http://www.us-cert.gov/cas/techalerts/TA07-290A.html

* FRSIRT: ADV-2007-3524
http://www.frsirt.com/english/advisories/2007/3524
* SECTRACK: 1018823
http://www.securitytracker.com/id?1018823
* SECUNIA: 27251
http://secunia.com/advisories/27251

CVE Reference: CVE-2007-5525

❖ 16675 Oracle Application Server - Oracle Single Sign-On component unspecified Vulnerability (oct-2007/AS09)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Single Sign-On component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html
* CERT: TA07-290A
http://www.us-cert.gov/cas/techalerts/TA07-290A.html
* FRSIRT: ADV-2007-3524
http://www.frsirt.com/english/advisories/2007/3524
* SECTRACK: 1018823
http://www.securitytracker.com/id?1018823
* SECUNIA: 27251
http://secunia.com/advisories/27251

CVE Reference: CVE-2007-5524

❖ 16674 Oracle Application Server - Oracle Internet Directory component unspecified Vulnerability (oct-2007/AS08)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Internet Directory component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html
* CERT: TA07-290A

http://www.us-cert.gov/cas/techalerts/TA07-290A.html
* FRSIRT: ADV-2007-3524
http://www.frsirt.com/english/advisories/2007/3524
* SECTRACK: 1018823
http://www.securitytracker.com/id?1018823
* SECUNIA: 27251
http://secunia.com/advisories/27251

CVE Reference: CVE-2007-5523

❖ 16673 Oracle Application Server - Oracle Portal component unspecified Vulnerability (oct-2007/AS07)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Portal component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html
* CERT: TA07-290A
http://www.us-cert.gov/cas/techalerts/TA07-290A.html
* FRSIRT: ADV-2007-3524
http://www.frsirt.com/english/advisories/2007/3524
* SECTRACK: 1018823
http://www.securitytracker.com/id?1018823
* SECUNIA: 27251
http://secunia.com/advisories/27251

CVE Reference: CVE-2007-5522

❖ 16672 Oracle Application Server - Oracle Containers for J2EE component unspecified Vulnerability (oct-2007/AS06)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Containers for J2EE component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html
* CERT: TA07-290A
http://www.us-cert.gov/cas/techalerts/TA07-290A.html
* FRSIRT: ADV-2007-3524

http://www.frsirt.com/english/advisories/2007/3524
* SECTRACK: 1018823
http://www.securitytracker.com/id?1018823
* SECUNIA: 27251
http://secunia.com/advisories/27251

CVE Reference: CVE-2007-5521

❖ 16671 Oracle Application Server - Oracle Internet Directory component unspecified Vulnerability (oct-2007/AS05)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Internet Directory component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html
* CERT: TA07-290A
http://www.us-cert.gov/cas/techalerts/TA07-290A.html
* FRSIRT: ADV-2007-3524
http://www.frsirt.com/english/advisories/2007/3524
* SECTRACK: 1018823
http://www.securitytracker.com/id?1018823
* SECUNIA: 27251
http://secunia.com/advisories/27251

CVE Reference: CVE-2007-5520

❖ 16670 Oracle Application Server - Oracle Portal component unspecified Vulnerability (oct-2007/AS04)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Portal component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html
* CERT: TA07-290A
http://www.us-cert.gov/cas/techalerts/TA07-290A.html
* FRSIRT: ADV-2007-3524
http://www.frsirt.com/english/advisories/2007/3524
* SECTRACK: 1018823
http://www.securitytracker.com/id?1018823
* SECUNIA: 27251

http://secunia.com/advisories/27251

CVE Reference: CVE-2007-5519

❖ 16669 Oracle Application Server - Oracle HTTP Server component unspecified Vulnerability (oct-2007/AS03)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle HTTP Server component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html
* CERT: TA07-290A
http://www.us-cert.gov/cas/techalerts/TA07-290A.html
* FRSIRT: ADV-2007-3524
http://www.frsirt.com/english/advisories/2007/3524
* SECTRACK: 1018823
http://www.securitytracker.com/id?1018823
* SECUNIA: 27251
http://secunia.com/advisories/27251

CVE Reference: CVE-2007-5518

❖ 16668 Oracle Application Server - Oracle Portal component unspecified Vulnerability (oct-2007/AS02)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Portal component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html
* CERT: TA07-290A
http://www.us-cert.gov/cas/techalerts/TA07-290A.html
* FRSIRT: ADV-2007-3524
http://www.frsirt.com/english/advisories/2007/3524
* SECTRACK: 1018823
http://www.securitytracker.com/id?1018823
* SECUNIA: 27251
http://secunia.com/advisories/27251

CVE Reference: CVE-2007-5517

New Vulnerabilities found this Week

Adobe Flash Player Multiple Vulnerabilities

"gain escalated privileges; cross-site scripting; disclose sensitive information; Denial of Service"

Some vulnerabilities have been reported in Adobe Flash Player, where one vulnerability has an unknown impact and others can be exploited by malicious, local users to gain escalated privileges and by malicious people to bypass certain security restrictions, conduct cross-site scripting and HTTP request splitting attacks, disclose sensitive information, cause a Denial of Service (DoS), or to potentially compromise a user's system.

1) An error when parsing specially crafted regular expressions can be exploited to cause a heap-based buffer overflow.

2) An error exists in the processing of SWF embedded JPG images. This can be exploited to corrupt the heap via specially crafted X and Y densities specified in the JPG header.

3) An error exists when pinning a hostname to an IP address. This can be exploited to conduct DNS rebinding attacks via allow-access-from elements in cross-domain-policy XML documents.

4) An error exists in the enforcing of cross-domain policy files. This can be exploited to bypass certain security restrictions on web servers hosting cross-domain policy files.

5) Input passed to unspecified parameters when handling the "asfunction:" protocol is not properly sanitized before being returned to the user. This can be exploited to inject arbitrary HTML and script code in a user's browser session in context of an affected site.

The vulnerability does not affect Flash Player 7.

6) An error exists within the processing of the "navigateToURL" function. This can be exploited to execute arbitrary script code in the security context of another domain via a specially crafted "javascript:" URI.

The vulnerability only affects the Flash Player ActiveX Control for Internet Explorer.

7) An unspecified error can be exploited to modify HTTP headers and conduct HTTP request splitting attacks.

8) An error within the implementation of the Socket or XMLSocket ActionScript classes can be exploited to determine if a port on a remote host is opened or closed.

9) An error within the setting of memory permissions in Adobe Flash Player for Linux can be exploited by malicious, local users to gain escalated privileges.

10) An unspecified error exists in Adobe Flash Player and Opera on Mac OS X.

The vulnerabilities are reported in versions prior to 9.0.115.0.

References:
http://www.adobe.com/support/security/bulletins/apsb07-20.html

Google Toolbar Custom Button Installer Dialog Spoofing Weakness

"spoofing attacks"

Aviv Raffon has discovered a weakness in Google Toolbar, which can be exploited by malicious people to conduct spoofing attacks.

The weakness is caused due to an error when handling domains that are being displayed in the Custom Button Installer dialog. This can be exploited to spoof the origin of a custom button and the domain information in the "privacy considerations" section via a specially crafted xml file in combination with a redirector page.

The weakness is confirmed in Google Toolbar version 4.0.1601.4987 for Internet Explorer. Other versions may also be affected.

References:
http://aviv.raffon.net/2007/12/18/GoogleToolbarDialogSpoofingVulnerability.aspx

HP-UX rpc.yppasswdd Unspecified Denial of Service Vulnerability

"Denial of Service"

A vulnerability has been reported in HP-UX, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error and can be exploited to crash the rpc.yppasswdd process. No further information is currently available.

The vulnerability affects HP-UX B.11.11, B.11.23 and B.11.31.

References:
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01294324

Cisco Firewall Services Module Denial of Service Vulnerability

"Denial of Service"

A vulnerability has been reported in the Cisco Firewall Services Module (FWSM), which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error in the processing of data in the control-plane path with Layer 7 Application Inspections. This can be exploited to cause a crash and reload the FWSM via specially crafted network traffic.

The vulnerability is reported in FWSM System Software version 3.2(3).

References:
http://www.cisco.com/warp/public/707/cisco-sa-20071219-fwsm.shtml

Thunderbird Multiple Vulnerabilities
"execute arbitrary code"

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

1) An error related to URI handlers potentially allows to execute arbitrary code.

2) Various errors in the browser engine and the Javascript engine can potentially be exploited by malicious people to compromise a user's system.

The vulnerabilities are reported in versions prior to 1.5.0.14.

References:
http://www.mozilla.org/security/announce/2007/mfsa2007-29.html
http://www.mozilla.org/security/announce/2007/mfsa2007-40.html

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