netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 6

February 8, 2008

Table of Contents

Product Focus

RPC DCOM Vulnerabilities Scanner – The RPC DCOM Vulnerabilities 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 Microsoft Windows RPC DCOM flaws (MS03-026 and MS03-039).

Check out our video section for a number of interviews with Jesper Jurcenoks: www.netvigilance.com/videos

This Week in Review

Grid computing faces challenges. PCI webinar for merchants. Retailers lack strategy. Google worries IT managers.

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

❖ Grid Computing Now! Grid Security

In the previous article in this series, Grid and licensing, Quocirca identified licensing issues as an obstacle to the widespread adoption of grid computing. This article looks at the critical and challenging issue of security in grid computing. Although providing enormous opportunity in terms of resource sharing and maximizing utilisation, running applications in grid environments gives rise to different types of security issues.

A compute grid is essentially a collection of distributed computing resources, aggregated to act as a unified processing resource or virtual supercomputer. Collecting these compute resources into a unified pool involves not only coordinated usage policies, job scheduling and queuing characteristics but also grid-wide security and user authentication. The first phase of grid computing evolution tends to be the creation of intra-grids; two or three clusters may be interconnected between departments within an enterprise to increase processing capacity and share data sets. Because the clusters are within one enterprise domain, things like security and authentication, although still important, are not so critical.

quocirca

Full Story :
http://www.quocirca.com/pages/analysis/articles/view/store251/item20761/

❖ PCI Security Standards Council To Host Webinar on Latest Self Assessment Questionnaire

Merchants and service providers to gain insight into latest tool for PCI self assessment
The PCI Security Standards Council, a global, open industry standards body providing management of the Payment Card Industry Data Security Standard (DSS), PCI PIN Entry Device (PED) Security Requirements and the Payment Application Data Security Standard (PA-DSS), today announces a complimentary webinar, “Navigating and Understanding the PCI SSC Self Assessment Questionnaire,” to be held on Thursday Feb. 21, 2008 at 11:30 a.m. EST and a second session the same day at 7:30 p.m. EST.

businesswire

Full Story :
http://www.businesswire.com/portal/site/newsnow/index.jsp?ndmViewId=news_view&ndmConfigId=1004993&newsId=20080207005395&newsLang=en

❖ Retailers need to step up IT security, says Deloitte

Retailers are losing the battle against IT security threats because most have no strategy for their long term defence and merely respond to incidents, says a report from management consultancy Deloittes.

"Consumer businesses have a tactical rather than a strategic approach to security," the company said. "This means they do not develop the foresight that allows them to deal with issues before they become problems."

The survey of managers responsible for IT security in consumer businesses such as retailers and consumer goods companies found 80% had no clear IT security strategy, but 93% had appointed someone to take responsibility for it.

Computerweekly

Full Story :

http://www.computerweekly.com/Articles/2008/02/07/229303/retailers-need-to-step-up-it-security-says-deloitte.htm

- **Free Google hosted applications sidestep IT department, raise security concerns**

This offering means IT managers who fret about employees using unauthorized software at work will have another tool to worry about especially in industries where information management is heavily regulated.
Google is releasing a new edition of its hosted applications suite that end-users can bring into the workplace without the involvement of their IT department.
It means that IT managers who fret about employees using unauthorized software at work will have another tool to worry about, especially in industries where information management is heavily regulated, like health care and finance.

itbusiness

Full Story :
http://www.itbusiness.ca/it/client/en/Home/News.asp?id=47046

New Vulnerabilities Tested in SecureScout

- **16849 QuickTime heap buffer overflow exists in QuickTime's handling of HTTP responses when RTSP tunneling is enabled (Remote File Checking)**

A heap buffer overflow exists in QuickTime's handling of HTTP responses when RTSP tunneling is enabled. By enticing a user to visit a maliciously crafted webpage, an attacker may cause an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.4.1.

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

References:

* BUGTRAQ: 20080110 Buffer-overflow in Quicktime Player 7.3.1.70
http://www.securityfocus.com/archive/1/archive/1/486091/100/0/threaded
* BUGTRAQ: 20080110 Re: Buffer-overflow in Quicktime Player 7.3.1.70
http://www.securityfocus.com/archive/1/archive/1/486114/100/0/threaded
* BUGTRAQ: 20080111 Re: Buffer-overflow in Quicktime Player 7.3.1.70
http://www.securityfocus.com/archive/1/archive/1/486174/100/0/threaded
* BUGTRAQ: 20080111 Re: Re: Buffer-overflow in Quicktime Player 7.3.1.70
http://www.securityfocus.com/archive/1/archive/1/486161/100/0/threaded
* BUGTRAQ: 20080112 Re: Buffer-overflow in Quicktime Player 7.3.1.70
http://www.securityfocus.com/archive/1/archive/1/486268/100/0/threaded
* BUGTRAQ: 20080112 Re: Re: Buffer-overflow in Quicktime Player 7.3.1.70
http://www.securityfocus.com/archive/1/archive/1/486241/100/0/threaded
* BUGTRAQ: 20080114 Re: [Full-disclosure] Buffer-overflow in Quicktime Player 7.3.1.70

http://www.securityfocus.com/archive/1/archive/1/486238/100/0/threaded
* MILW0RM: 4885
http://www.milw0rm.com/exploits/4885
* MILW0RM: 4906
http://www.milw0rm.com/exploits/4906
* CERT-VN: VU#112179
http://www.kb.cert.org/vuls/id/112179
* BID: 27225
http://www.securityfocus.com/bid/27225
* FRSIRT: ADV-2008-0107
http://www.frsirt.com/english/advisories/2008/0107
* SECTRACK: 1019178
http://www.securitytracker.com/id?1019178
* SECUNIA: 28423
http://secunia.com/advisories/28423
* XF: quicktime-rtsp-responses-bo(39601)
http://xforce.iss.net/xforce/xfdb/39601

CVE Reference: CVE-2008-0234

❖ 16848 QuickTime integer arithmetic issue in QuickTime's handling of certain movie file atoms may lead to a stack buffer overflow (Remote File Checking)

An integer arithmetic issue in QuickTime's handling of certain movie file atoms may lead to a stack buffer overflow. By enticing a user to open a maliciously crafted movie file, an attacker may cause an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.3.0.

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

References:

* BUGTRAQ: 20071114 TPTI-07-20: Apple Quicktime Movie Stack Overflow Vulnerability
http://www.securityfocus.com/archive/1/archive/1/483717/100/100/threaded
* MISC:
http://dvlabs.tippingpoint.com/advisory/TPTI-07-20
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=306896

CVE Reference: CVE-2007-4674

❖ 16847 QuickTime heap buffer overflow exists in the parsing of the color table atom when opening a movie file (Remote File Checking)

A heap buffer overflow exists in the parsing of the color table atom when opening a movie file. By enticing a user to open a maliciously crafted movie file, an attacker may cause an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.3.0.

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

References:

* BUGTRAQ: 20071105 ZDI-07-065: Apple QuickTime Color Table RGB Parsing Heap Corruption Vulnerability
http://www.securityfocus.com/archive/1/archive/1/483312/100/0/threaded
* MISC:
http://www.zerodayinitiative.com/advisories/ZDI-07-065.html
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=306896
* APPLE: APPLE-SA-2007-11-05
http://lists.apple.com/archives/Security-announce/2007/Nov/msg00000.html
* CERT: TA07-310A
http://www.us-cert.gov/cas/techalerts/TA07-310A.html
* CERT-VN: VU#445083
http://www.kb.cert.org/vuls/id/445083
* BID: 26338
http://www.securityfocus.com/bid/26338
* FRSIRT: ADV-2007-3723
http://www.frsirt.com/english/advisories/2007/3723
* OSVDB: 38544
http://www.osvdb.org/38544
* SECTRACK: 1018894
http://www.securitytracker.com/id?1018894
* SECUNIA: 27523
http://secunia.com/advisories/27523
* SREASON: 3352
http://securityreason.com/securityalert/3352
* XF: quicktime-colortable-atom-bo(38283)
http://xforce.iss.net/xforce/xfdb/38283

CVE Reference: CVE-2007-4677

❖ 16846 QuickTime heap buffer overflow exists in QuickTime's handling of panorama sample atoms in QTVR (QuickTime Virtual Reality) movie files (Remote File Checking)

A heap buffer overflow exists in QuickTime's handling of panorama sample atoms in QTVR (QuickTime Virtual Reality) movie files. By enticing a user to view a maliciously crafted QTVR file, an attacker may cause an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.3.0.

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

References:

* IDEFENSE: 20071105 Apple QuickTime Panorama Sample Atom Heap Buffer Overflow Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=620
* BUGTRAQ: 20071110 [48Bits Advisory] QuickTime Panorama Sample Atom Heap Overflow
http://www.securityfocus.com/archive/1/archive/1/483564/100/0/threaded
* MISC:
http://blog.48bits.com/?p=176
* MISC:
http://www.48bits.com/advisories/qt_pdat_heapbof.pdf
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=306896
* APPLE: APPLE-SA-2007-11-05
http://lists.apple.com/archives/Security-announce/2007/Nov/msg00000.html
* CERT: TA07-310A
http://www.us-cert.gov/cas/techalerts/TA07-310A.html
* BID: 26342
http://www.securityfocus.com/bid/26342
* FRSIRT: ADV-2007-3723
http://www.frsirt.com/english/advisories/2007/3723
* OSVDB: 38545
http://www.osvdb.org/38545
* SECTRACK: 1018894
http://www.securitytracker.com/id?1018894
* SECUNIA: 27523
http://secunia.com/advisories/27523
* XF: quicktime-qtvr-bo(38282)
http://xforce.iss.net/xforce/xfdb/38282

CVE Reference: CVE-2007-4675

❖ 16845 QuickTime heap buffer overflow exists in PICT image processing (Remote File Checking)

A heap buffer overflow exists in PICT image processing. By enticing a user to open a maliciously crafted image, an attacker may cause an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.3.0.

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

References:

* BUGTRAQ: 20071105 ZDI-07-066: Apple Quicktime PICT File PackBitsRgn Parsing Heap Corruption Vulnerability

http://www.securityfocus.com/archive/1/archive/1/483311/100/0/threaded
* BUGTRAQ: 20071105 ZDI-07-067: Apple QuickTime PICT File Poly Opcodes Heap Corruption Vulnerability
http://www.securityfocus.com/archive/1/archive/1/483313/100/0/threaded
* MISC:
http://www.zerodayinitiative.com/advisories/ZDI-07-066.html
* MISC:
http://www.zerodayinitiative.com/advisories/ZDI-07-067.html
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=306896
* APPLE: APPLE-SA-2007-11-05
http://lists.apple.com/archives/Security-announce/2007/Nov/msg00000.html
* CERT: TA07-310A
http://www.us-cert.gov/cas/techalerts/TA07-310A.html
* CERT-VN: VU#690515
http://www.kb.cert.org/vuls/id/690515
* BID: 26345
http://www.securityfocus.com/bid/26345
* FRSIRT: ADV-2007-3723
http://www.frsirt.com/english/advisories/2007/3723
* SECTRACK: 1018894
http://www.securitytracker.com/id?1018894
* SECUNIA: 27523
http://secunia.com/advisories/27523
* SREASON: 3351
http://securityreason.com/securityalert/3351
* XF: quicktime-packbitsrgn-bo(38280)
http://xforce.iss.net/xforce/xfdb/38280
* XF: quicktime-poly-type-bo(38281)
http://xforce.iss.net/xforce/xfdb/38281

CVE Reference: CVE-2007-4676

❖ 16844 QuickTime stack buffer overflow exists in PICT image processing (Remote File Checking)

A stack buffer overflow exists in PICT image processing. By enticing a user to open a maliciously crafted image, an attacker may cause an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.3.0.

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

References:

* BUGTRAQ: 20071105 ZDI-07-068: Apple QuickTime Uncompressedfile Opcode Stack Overflow Vulnerability
http://www.securityfocus.com/archive/1/archive/1/483314/100/0/threaded
* MISC:
http://www.zerodayinitiative.com/advisories/ZDI-07-068.html
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=306896

* APPLE: APPLE-SA-2007-11-05
http://lists.apple.com/archives/Security-announce/2007/Nov/msg00000.html
* CERT: TA07-310A
http://www.us-cert.gov/cas/techalerts/TA07-310A.html
* BID: 26344
http://www.securityfocus.com/bid/26344
* FRSIRT: ADV-2007-3723
http://www.frsirt.com/english/advisories/2007/3723
* SECTRACK: 1018894
http://www.securitytracker.com/id?1018894
* SECUNIA: 27523
http://secunia.com/advisories/27523
* SREASON: 3350
http://securityreason.com/securityalert/3350
* XF: apple-quicktime-pict-bo(38279)
http://xforce.iss.net/xforce/xfdb/38279

CVE Reference: CVE-2007-4672

❖ 16724 Oracle Application Server - OC4J component unspecified Vulnerability (jul-2006/AS03)

An unspecified vulnerability with unknown impact exists in Oracle Application Server OC4J component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/440758/100/100/threaded
* CERT: TA06-200A
http://www.us-cert.gov/cas/techalerts/TA06-200A.html
* BID: 19054
http://www.securityfocus.com/bid/19054
* FRSIRT: ADV-2006-2863
http://www.frsirt.com/english/advisories/2006/2863
* FRSIRT: ADV-2006-2947
http://www.frsirt.com/english/advisories/2006/2947
* SECTRACK: 1016529
http://securitytracker.com/id?1016529
* SECUNIA: 21111
http://secunia.com/advisories/21111
* SECUNIA: 21165
http://secunia.com/advisories/21165
* XF: oracle-cpu-july-2006(27897)
http://xforce.iss.net/xforce/xfdb/27897

CVE Reference: CVE-2006-3708

❖ 16723 Oracle Application Server - OC4J component unspecified Vulnerability (jul-2006/AS02)

An unspecified vulnerability with unknown impact exists in Oracle Application Server OC4J component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/440758/100/100/threaded
* CERT: TA06-200A
http://www.us-cert.gov/cas/techalerts/TA06-200A.html
* BID: 19054
http://www.securityfocus.com/bid/19054
* FRSIRT: ADV-2006-2863
http://www.frsirt.com/english/advisories/2006/2863
* FRSIRT: ADV-2006-2947
http://www.frsirt.com/english/advisories/2006/2947
* SECTRACK: 1016529
http://securitytracker.com/id?1016529
* SECUNIA: 21111
http://secunia.com/advisories/21111
* SECUNIA: 21165
http://secunia.com/advisories/21165
* XF: oracle-cpu-july-2006(27897)
http://xforce.iss.net/xforce/xfdb/27897

CVE Reference: CVE-2006-3707

❖ 16722 Oracle Application Server - OC4J component unspecified Vulnerability (jul-2006/AS01)

An unspecified vulnerability with unknown impact exists in Oracle Application Server OC4J component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html

* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/440758/100/100/threaded
* CERT: TA06-200A
http://www.us-cert.gov/cas/techalerts/TA06-200A.html
* BID: 19054
http://www.securityfocus.com/bid/19054
* FRSIRT: ADV-2006-2863
http://www.frsirt.com/english/advisories/2006/2863
* FRSIRT: ADV-2006-2947
http://www.frsirt.com/english/advisories/2006/2947
* SECTRACK: 1016529
http://securitytracker.com/id?1016529
* SECUNIA: 21111
http://secunia.com/advisories/21111
* SECUNIA: 21165
http://secunia.com/advisories/21165
* XF: oracle-cpu-july-2006(27897)
http://xforce.iss.net/xforce/xfdb/27897

CVE Reference: CVE-2006-3706

❖ 16721 Oracle Application Server - Oracle Containers for J2EE component unspecified Vulnerability (oct-2006/OC4J05)

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: **Low**

References:

* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_oct_2006.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/449711/100/0/threaded
* CERT: TA06-291A
http://www.us-cert.gov/cas/techalerts/TA06-291A.html
* BID: 20588
http://www.securityfocus.com/bid/20588
* FRSIRT: ADV-2006-4065
http://www.frsirt.com/english/advisories/2006/4065
* SECTRACK: 1017077
http://securitytracker.com/id?1017077
* SECUNIA: 22396
http://secunia.com/advisories/22396

CVE Reference: CVE-2006-5364

New Vulnerabilities found this Week

Skype Cross-Zone Scripting Security Enhancement

"script insertion"

An update has been released for Skype, which implements security enhancements to prevent compromise of users' systems.

Skype uses the Internet Explorer web control to render HTML from certain websites (e.g. DailyMotion, Metacafe, and SkypeFind). As the content is rendered in the "Local Machine" security zone, this allows execution of arbitrary script code on a user's system via script insertion vulnerabilities present in these websites.

Various vulnerabilities have been discovered in these sites, which provide vectors when a user e.g. uses the Skype video gallery browser section or finds a video uploaded to the DailyMotion gallery with a specially crafted video title.

Successful exploitation requires that a displayed website is vulnerable to
The vulnerability is reported in the following Skype for Windows versions:
- All versions including 3.5.*
- Version 3.6.*.244 and prior

References:
http://www.skype.com/security/skype-sb-2008-001-update2.html
http://www.skype.com/intl/en/security/skype-sb-2008-002.html
http://www.skype.com/intl/en/security/skype-sb-2008-001-update1.html
http://www.skype.com/intl/en/security/skype-sb-2008-001.html

Sun JRE Applet Handling Two Vulnerabilities

"execute local applications"

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

The vulnerabilities are caused due to unspecified errors within the handling of Java applets. These can be exploited by malicious, untrusted applets to read and write local files, or to execute local applications.

The vulnerabilities are reported in the following products (for Windows, Solaris, and Linux):
* JDK and JRE 6 Update 1 and earlier
* JDK and JRE 5.0 Update 13 and earlier

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-66-231261-1

OpenBSD DNS Server PRNG Transaction ID Vulnerability

"poison the DNS cache"

Amit Klein has reported a vulnerability in OpenBSD, which can be exploited by malicious people to poison the DNS cache.

The vulnerability is caused due to a weakness within the OpenBSD DNS server's pseudo random number generator (PRNG). This can be exploited to obtain the DNS transaction ID and poison the DNS cache.

The vulnerability is reported in OpenBSD versions 3.3 to 4.2.

References:
http://www.trusteer.com/docs/dnsopenbsd.html

Symantec Backup Exec System Recovery Manager File Upload Vulnerability

"upload arbitrary files"

A vulnerability has been reported in Symantec Backup Exec System Recovery Manager, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an error within the FileUpload class running on the Symantec LiveState Apache Tomcat server. This can be exploited to upload arbitrary files via a specially crafted HTTP POST request.

Successful exploitation allows execution of arbitrary code.

The vulnerability is reported in versions 7.0 and 7.0.1.

References:
http://seer.entsupport.symantec.com/docs/297171.htm

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