netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 16

April 18, 2008

Table of Contents

Product Focus

Much anticipated "Negev" in public Beta.

Try the New Beta Perimeter system, our Web-interface for the Perimeter Service is now running dynamic pages based on "Ajax", giving a much improved response time and customer experience. Existing customers can log right into the new system from the usual login page, The rest of you should contact sales for a free trial.

Nimda Worm Scanner – The Nimda Worm 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 MS IE Mime Header Flaw (MS01-020) or have been infected by the Nimda Worm.

CTO Jesper Jurcenoks of netVigilance is the keynote speaker at the ITEC Conference & Exhibition 2008 in Houston May 8, see
http://www.netvigilance.com/events

This Week in Review

Panel discussion warns of global cubertrust collapse. Next target may be the processor itself. PCI takes over VISA security standard. Protecting client data in cyberspace.

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

❖ From RSA: Today's risk model isn't working, Jericho Forum panel agrees

Without a fundamental transformation in the way organizations perceive, execute and manage risk, a global collapse of cybertrust would make America's subprime mortgage mess look like a picnic, said Adrian Seccombe, CISO and senior enterprise architect at Eli Lilly.

Seccombe was addressing a group of about 30 IT luminaries during a half-day collaborative panel discussion around de-perimeterization on Thursday afternoon hosted by the Jericho Forum, a think tank of IT executives from public and private sector companies. He advocated a security "trust" model that looks at security radically different than today's current, outside-in risk models.

scmagazine

Full Story :
http://www.scmagazineus.com/From-RSA-Todays-risk-model-isnt-working-Jericho-Forum-panel-agrees/article/108963/

❖ Hacking microprocessors is the next step

HACKING SOFTWARE TO gain access to someone else's computer could soon become "old school", according to boffins at the University of Illinois, who say that the next level for hackers is hacking the microprocessor itself.

New research has shown that it is in fact possible to alter chips in such a way as to leave computers helpless to back-door attacks, which would be almost impossible to detect.To prove their point, researchers set up a demo of such an attack yesterday, in San Francisco, at a security conference called the Usenix Workshop on Large-Scale Exploits and Emergent Threats. The alarming demo showed how a processor running a Linux operating system was left totally vulnerable after a malicious firmware laden chip was given instructions to allow an attacker to log on to the computer without any trouble at all.

The inquirer

Full Story :
http://www.theinquirer.net/gb/inquirer/news/2008/04/16/hacking-microprocessors-step

❖ PCI council unveils payment application standard

The Payment Card Industry (PCI) Security Standards Council has officially taken over control of a new data security standard from Visa.

The council announced on Tuesday that it is making available version 1.1 of the PA-DSS (Payment Application Data Security Standard) to complement two other standards it already administers -- the well-known PCI-DSS, a 12-step mandate for safeguarding credit

card information, and the PCI PIN Entry Device (PED) standard, which governs devices that accept Visa or MasterCard PINs.

scmagazine

Full Story :
http://www.scmagazineus.com/PCI-council-unveils-payment-application-standard/article/109097/

The legal security blanket

Law firms the world over have founded their success on the maxim 'knowledge is power'. By the very nature of their business, lawyers occupy an enormously privileged position, being privy to the confidential documents, private conversations and sensitive information essential to commercial life. Yet with great power comes great responsibility, especially as we move into a position where the bulk of this information takes electronic form.

Protecting client confidentiality is holy writ for the profession, but how can we square this need for secrecy with a world in which a critical document concerning an initial public offering or an acquisition can be emailed to someone in the blink of an eye? We need look no further than the headlines to see the chaos that lax IT security policies can lead to: whether this be 24 million child benefit records copied to CDs and lost in the post, or the website of a major broadsheet newspaper (the Telegraph) brought down by hackers.

legalweek

Full Story :
http://www.legalweek.com/Navigation/33/Articles/1116349/The+legal+security+blanket.html

New Vulnerabilities Tested in SecureScout

- **13619 Oracle Database Server - Advanced Queuing component unspecified Vulnerability (apr-2008/DB01)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Advanced Queuing" component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html
* SECUNIA: 29829
http://secunia.com/advisories/29829/

CVE Reference:

CVE-2008-1813 (cve.mitre.org, nvd.nist.gov)

- **13620 Oracle Database Server - Change Data Capture component unspecified Vulnerability (apr-2008/DB02)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Change Data Capture" component.

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

References:

* SECUNIA: 29829
http://secunia.com/advisories/29829/
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html

CVE Reference:

CVE-2008-1815 (cve.mitre.org, nvd.nist.gov)

- **13621 Oracle Database Server - Core RDBMS component unspecified Vulnerability (apr-2008/DB03)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Core RDBMS" component.

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

References:

* SECUNIA: 29829
http://secunia.com/advisories/29829/
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html

CVE Reference:

CVE-2008-1813 (cve.mitre.org, nvd.nist.gov)

- **13622 Oracle Database Server - Oracle Secure Enterprise Search or Ultrasearch component unspecified Vulnerability (apr-2008/DB04)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Oracle Secure Enterprise Search or Ultrasearch" component.

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

References:

* SECUNIA: 29829
http://secunia.com/advisories/29829/
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html

CVE Reference:

CVE-2008-1814 (cve.mitre.org, nvd.nist.gov)

- **13623 Oracle Database Server - Oracle Spatial component SQL injection Vulnerability (apr-2008/DB05)**

An SQL injection vulnerability exists in Oracle Database Server "Oracle Spatial" component.

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

References:

* SECUNIA: 29829
http://secunia.com/advisories/29829/
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html
* MISC:
http://www.red-database-security.com/advisory/oracle_sql_injection_sdo_util.html

CVE Reference:

CVE-2008-1816 (cve.mitre.org, nvd.nist.gov)

- **13624 Oracle Database Server - Oracle Spatial component SQL injection Vulnerability (apr-2008/DB06)**

An SQL injection vulnerability exists in Oracle Database Server "Oracle Spatial" component.

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

References:

* SECUNIA: 29829
http://secunia.com/advisories/29829/
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html
* MISC:
http://www.red-database-security.com/advisory/oracle_sql_injection_sdo_geom.html

CVE Reference:

CVE-2008-1813 (cve.mitre.org, nvd.nist.gov)

- **13625 Oracle Database Server - Oracle Spatial component SQL injection Vulnerability (apr-2008/DB07)**

An SQL injection vulnerability exists in Oracle Database Server "Oracle Spatial" component.

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

References:

* SECUNIA: 29829
http://secunia.com/advisories/29829/
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html
* MISC:
http://www.red-database-security.com/advisory/oracle_sql_injection_sdo_idx.html

CVE Reference:

CVE-2008-1817 (cve.mitre.org, nvd.nist.gov)

- **13626 Oracle Database Server - Authentication component unspecified Vulnerability (apr-2008/DB08)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Authentication" component.

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

References:

* SECUNIA: 29829
http://secunia.com/advisories/29829/
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html

CVE Reference:

CVE-2008-1818 (cve.mitre.org, nvd.nist.gov)

- **13627 Oracle Database Server - Oracle Net Services component unspecified Vulnerability (apr-2008/DB09)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Oracle Net Services" component.

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

References:

* SECUNIA: 29829
http://secunia.com/advisories/29829/
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html

CVE Reference:

CVE-2008-1819 (cve.mitre.org, nvd.nist.gov)

- **13628 Oracle Database Server - Core RDBMS component unspecified Vulnerability (apr-2008/DB10)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Core RDBMS" component.

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

References:

* SECUNIA: 29829
http://secunia.com/advisories/29829/
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html

CVE Reference:

CVE-2008-1817 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

Oracle Products Multiple Vulnerabilities

"SQL injection attacks; Denial of Service; compromise a vulnerable system"

Multiple vulnerabilities have been reported for various Oracle products. Some vulnerabilities have unknown impacts while others can be exploited by malicious users to bypass certain security restrictions, conduct SQL injection attacks, cause a DoS (Denial of Service), or potentially compromise a vulnerable system.

The vulnerabilities are reported in the following products and versions:
* Oracle Database 11g, version 11.1.0.6
* Oracle Database 10g Release 2, versions 10.2.0.2, 10.2.0.3
* Oracle Database 10g, version 10.1.0.5
* Oracle Database 9i Release 2, versions 9.2.0.8, 9.2.0.8DV
* Oracle Application Server 10g Release 3 (10.1.3), versions 10.1.3.1.0, 10.1.3.3.0
* Oracle Application Server 10g Release 2 (10.1.2), versions 10.1.2.0.2, 10.1.2.1.0, 10.1.2.2.0

* Oracle Application Server 10g (9.0.4), version 9.0.4.3
* Oracle Collaboration Suite 10g, version 10.1.2
* Oracle E-Business Suite Release 12, version 12.0.4
* Oracle E-Business Suite Release 11i, version 11.5.10.2
* Oracle PeopleSoft Enterprise PeopleTools versions 8.22.19, 8.48.16, 8.49.09
* Oracle PeopleSoft Enterprise HCM versions 8.8 SP1, 8.9, 9.0
* Oracle Siebel SimBuilder versions 7.8.2, 7.8.5

References:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2008.html

ClamAV Multiple Vulnerabilities

"Denial of Service; Execution of arbitrary code"

Some vulnerabilities have been reported in ClamAV, which can be exploited by malicious people to cause a DoS (Denial of Service) or to compromise a vulnerable system.

1) A boundary error exists within the "cli_scanpe()" function in libclamav/pe.c. This can be exploited to cause a heap-based buffer overflow via a specially crafted "Upack" executable.

Successful exploitation allows execution of arbitrary code.

2) A boundary error within the processing of PeSpin packed executables in libclamav/spin.c can be exploited to cause a heap-based buffer overflow.

Successful exploitation may allow execution of arbitrary code.

3) An unspecified error in the processing of ARJ files can be exploited to hang ClamAV.

4) A boundary error within the processing of WWPack packed PE files in libclamav/pe.c can be exploited to cause a heap corruption.

Successful exploitation may allow execution of arbitrary code.

The vulnerabilities are reported in version 0.92.1. Prior versions may also be affected.
References:
https://www.clamav.net/bugzilla/show_bug.cgi?id=878
https://www.clamav.net/bugzilla/show_bug.cgi?id=876
https://www.clamav.net/bugzilla/show_bug.cgi?id=897
https://www.clamav.net/bugzilla/show_bug.cgi?id=877

DivX Player Subtitle Parsing Buffer Overflow Vulnerability

"Execution of arbitrary code"

securfrog has discovered a vulnerability in DivX Player, which can potentially be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the processing of subtitles. This can be exploited to cause a stack-based buffer overflow via an overly long subtitle line contained in a malicious SRT file.

Successful exploitation may allow execution of arbitrary code, but requires that the user is tricked into opening a specially crafted SRT file.

The vulnerability is confirmed in DivX Player 6.7 (build 6.7.0.22). Other versions may also be affected.

References:
http://milw0rm.com/exploits/5453

VMware ESX Server Multiple Security Updates

"Denial of Service; Disclose sensitive information; compromise a vulnerable system"

VMware has issued an update for VMware ESX Server. This fixes some vulnerabilities, which can be exploited by malicious people to cause a DoS (Denial of Service), disclose sensitive information, or potentially compromise a vulnerable system.

References:
http://lists.vmware.com/pipermail/security-announce/2008/000014.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