netVigilance
assurance has arrived

2007 Issue # 51

ScoutNews

The weekly Security update from the makers of SecureScout

December 28, 2007

Table of Contents

Product Focus

Apache Chunked Vulnerability Scanner – The Apache Chunked 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 Apache Chunked Encoding buffer overflow.

This Week in Review

Learn how to track spamming botnets. Datamining. Hackers prosper from online scanners. A look at AJAX 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

- **Kaspersky Lab releases a new article: “Coordinated distributions method for tracking botnets sending out spam”**

Kaspersky Lab, a leading developer of secure content management solutions, has released a new analytical article “Coordinated distributions method for tracking botnets sending out spam”. The author is Andrey Bakhmutov.

The article presents a new method to resist botnets, sending out spam. This is a method to automatically separate and block those networks in real time. The method uses a statistical approach exploiting the fact that computers in a botnet have to have some similarities in their behavior. By monitoring e-mail traffic from numerous sources over a period of time it is possible to notice that message streams from some of the sources share common characteristics which mark them out from the rest of the computers sending e-mail messages.

Viruslist.com

Full Story :
http://www.viruslist.com/en/analysis?pubid=204791978

❖ The Theory and Practice of Secure Data Mining

Data mining isn't always about structured data. Text mining -- or text data mining -- is about comprehending natural language and extracting high quality information from it. Natural languages have structure, too. These structures are generally more complex than a schema, especially one designed for data mining.
As you read a sentence, its meaning may be clear even before you reach its end. This illustrates our topic. Our minds process text sequentially. As we read, the context presented to us by an author develops in our minds.

TechnewsWorld

Full Story :
http://www.technewsworld.com/story/tech-security/60819.html

❖ Online scanners help virus writers, claims Kaspersky

Online virus scanners can actually help malware writers, according to leading security firm Kaspersky.

Sites such as VirusTotal and VirusScan allow users to check suspicious files against multiple antivirus databases.

However, Kaspersky claims the services have become a Frankenstein's Monster, with virus writers using them to check the effectiveness of their malware. "They quickly caught on to the fact that services like the ones mentioned above could be used to test how well their creations can evade popular antivirus solutions," the company claims on its VirusList blog.

PC Pro

Full Story :
http://www.pcpro.co.uk/news/150123/online-scanners-help-virus-writers-claims-kaspersky.html

❖ Advanced AJAX Security: A Closer Look

Billy Hoffman gave a talk on advanced AJAX security at the recent Google Web Toolkit (GWT) conference in San Francisco. Hoffman manages HP Security Labs, which was

SPIDynamics until HP acquired it this year, along with Hoffman. He focuses on automated discovery of Web application vulnerabilities and Web crawling technologies.

His research includes areas such as sampling, JavaScript static analysis (automatic analysis of source code), and cross-site scripting (XSS) -- code injection by malicious Web users into Web pages viewed by other users. However, he did note that XSS isn't required for AJAX hacking; there's much lower-hanging fruit.

Enterprise ystems

Full Story :
http://www.esj.com/newswire/article.aspx?EditorialsID=2939

New Vulnerabilities Tested in SecureScout

❖ 16689 Oracle Application Server - Oracle Workflow Cartridge component unspecified Vulnerability (apr-2007/OWF01)

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

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

References:

* MISC:
http://www.integrigy.com/security-resources/analysis/Integrigy_Oracle_CPU_April_2007_Analysis.pdf
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/466329/100/200/threaded
* BID: 23532
http://www.securityfocus.com/bid/23532
* FRSIRT: ADV-2007-1426
http://www.frsirt.com/english/advisories/2007/1426
* SECTRACK: 1017927
http://www.securitytracker.com/id?1017927

CVE Reference: CVE-2007-2130

❖ 16688 Oracle Application Server - Oracle Portal (Ultra Search) and Oracle WebCenter Suite (Secure Enterprise Search) components unspecified Vulnerability (apr-2007/SES01)

An unspecified vulnerability with unknown impact exists in Oracle Application Server

Oracle Portal (Ultra Search) and Oracle WebCenter Suite (Secure Enterprise Search) components.

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

References:

* BUGTRAQ: 20070418 Advisory: XSS Vulnerability in Oracle Secure Enterprise Search [SES01]
http://www.securityfocus.com/archive/1/archive/1/466156/100/0/threaded
* MISC:
http://www.red-database-security.com/advisory/oracle_css_ses.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/466329/100/200/threaded
* BID: 23532
http://www.securityfocus.com/bid/23532
* FRSIRT: ADV-2007-1426
http://www.frsirt.com/english/advisories/2007/1426
* SECTRACK: 1017927
http://www.securitytracker.com/id?1017927

CVE Reference: CVE-2007-2119

❖ 16687 Oracle Application Server - Oracle Internet Directory component unspecified Vulnerability (jul-2007/OID01)

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:

* MISC:
http://www.integrigy.com/security-resources/analysis/Integrigy_Oracle_CPU_July_2007_Analysis.pdf
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* HP: HPSBMA02133
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?lang=en&cc=us&objectID=c00727143
* FRSIRT: ADV-2007-2562

http://www.frsirt.com/english/advisories/2007/2562
* FRSIRT: ADV-2007-2635
http://www.frsirt.com/english/advisories/2007/2635
* SECTRACK: 1018415
http://www.securitytracker.com/id?1018415
* SECUNIA: 26114
http://secunia.com/advisories/26114
* SECUNIA: 26166
http://secunia.com/advisories/26166
* XF: oracle-cpu-july2007(35490)
http://xforce.iss.net/xforce/xfdb/35490

CVE Reference: CVE-2007-3859

❖ 16685 Oracle Application Server - Oracle Portal component unspecified Vulnerability (apr-2007/AS05)

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:

* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/466329/100/200/threaded
* BID: 23532
http://www.securityfocus.com/bid/23532
* FRSIRT: ADV-2007-1426
http://www.frsirt.com/english/advisories/2007/1426
* SECTRACK: 1017927
http://www.securitytracker.com/id?1017927

CVE Reference: CVE-2007-2124

❖ 16684 Oracle Application Server - Oracle Portal component unspecified Vulnerability (apr-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:

* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/466329/100/200/threaded
* BID: 23532
http://www.securityfocus.com/bid/23532
* FRSIRT: ADV-2007-1426
http://www.frsirt.com/english/advisories/2007/1426
* SECTRACK: 1017927
http://www.securitytracker.com/id?1017927

CVE Reference: CVE-2007-2123

❖ 16683 Oracle Application Server - Oracle Wireless component unspecified Vulnerability (apr-2007/AS03)

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

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

References:

* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/466329/100/200/threaded
* BID: 23532
http://www.securityfocus.com/bid/23532
* FRSIRT: ADV-2007-1426
http://www.frsirt.com/english/advisories/2007/1426
* SECTRACK: 1017927
http://www.securitytracker.com/id?1017927

CVE Reference: CVE-2007-2122

❖ 16682 Oracle Application Server - Oracle COREid Access component unspecified Vulnerability (apr-2007/AS02)

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

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

References:

* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/466329/100/200/threaded
* BID: 23532
http://www.securityfocus.com/bid/23532
* FRSIRT: ADV-2007-1426
http://www.frsirt.com/english/advisories/2007/1426
* SECTRACK: 1017927
http://www.securitytracker.com/id?1017927

CVE Reference: CVE-2007-2121

❖ 16681 Oracle Application Server - Oracle Discoverer component unspecified Vulnerability (apr-2007/AS01)

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

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

References:

* BUGTRAQ: 20070418 Advisory: Shutdown unprotected Oracle TNS Listener via Oracle Discoverer Servlet [AS01]
http://www.securityfocus.com/archive/1/archive/1/466160/100/0/threaded
* MISC:
http://www.red-database-security.com/advisory/oracle_discoverer_servlet.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/466329/100/200/threaded
* BID: 23532
http://www.securityfocus.com/bid/23532
* FRSIRT: ADV-2007-1426
http://www.frsirt.com/english/advisories/2007/1426
* SECTRACK: 1017927
http://www.securitytracker.com/id?1017927

CVE Reference: CVE-2007-2120

❖ 16680 Oracle Application Server - Oracle Single Sign On component unspecified Vulnerability (jul-2007/AS01)

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:

* MISC:
http://www.integrigy.com/security-resources/analysis/Integrigy_Oracle_CPU_July_2007_Analysis.pdf
* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html
* HP: HPSBMA02133
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?lang=en&cc=us&objectID=c00727143
* FRSIRT: ADV-2007-2562
http://www.frsirt.com/english/advisories/2007/2562
* FRSIRT: ADV-2007-2635
http://www.frsirt.com/english/advisories/2007/2635
* SECTRACK: 1018415
http://www.securitytracker.com/id?1018415
* SECUNIA: 26114
http://secunia.com/advisories/26114
* SECUNIA: 26166
http://secunia.com/advisories/26166
* XF: oracle-cpu-july2007(35490)
http://xforce.iss.net/xforce/xfdb/35490

CVE Reference: CVE-2007-3862

❖ 15367 Oracle Application Server - Oracle Process Mgmt & Notification component unspecified Vulnerability (oct-2007/AS01)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Process Mgmt & Notification 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-2007-5516

New Vulnerabilities found this Week

Novell Identity Manager asampsp Denial of Service

"Denial of Service"

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

The vulnerability is caused due to a format string error and can be exploited to crash the Platform Service Process (asampsp) via specially crafted packets containing format specifiers.

The vulnerability is reported in version 3.5.1. Other versions may also be affected.

References:
http://support.novell.com/docs/Readmes/InfoDocument/patchbuilder/readme_5007560.html

Groove Virtual Office XUpload ActiveX Control Buffer Overflow

"Arbitrary code execution"

A vulnerability has been discovered in Groove Virtual Office, which can be exploited by malicious people to compromise a user's system.

The vulnerability is confirmed in version 3.1.1.2390. Other versions may also be affected.

References:
http://secunia.com/advisories/28145/

WinAce UUE File Decompression Buffer Overflow

"execution of arbitrary code"

A vulnerability has been reported in WinAce, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error when decompressing UUE files and can be exploited to cause a heap-based buffer overflow via a specially crafted UUE file containing an overly long filename.

Successful exploitation may allow execution of arbitrary code.

The vulnerability is reported in version 2.65. Other versions may also be affected.

References:
http://www.fourteenforty.jp/research/advisory.cgi?FFRRA-20071225

IBM HTTP Server Two Cross-Site Scripting Vulnerabilities

“cross-site scripting attacks”

IBM has acknowledged two vulnerabilities in IBM HTTP Server, which can be exploited by malicious people to conduct cross-site scripting attacks.

References:
http://www-1.ibm.com/support/docview.wss?uid=swg1PK57952
http://www-1.ibm.com/support/docview.wss?uid=swg1PK58024

IBM Lotus Domino Web Access Control ActiveX Control Buffer Overflow

“execution of arbitrary code”

A vulnerability has been reported in IBM Lotus Domino Web Access, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the dwa7.dwa7.1 ActiveX control (dwa7W.dll) when handling strings assigned to the "General_ServerName" property. This can be exploited to cause a stack-based buffer overflow by assigning an overly long string to the affected property and then calling the "InstallBrowserHelperDll()" method.

Successful exploitation allows execution of arbitrary code.

The vulnerability is reported in dwa7W.dll version 7.0.34.1 and reportedly affects IBM Lotus Domino 6.x and 7.x. Other versions may also be affected.

References:
http://lists.grok.org.uk/pipermail/full-disclosure/2007-December/059233.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