

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

[Sasser Worm Scanner](#) - The S4 Spida Digispid Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are prone any of the Microsoft Java Virtual Machine Vulnerabilities (MS02-069).

This Week in Review

SecureScout gets great review. Increased usage and security problems expected during OL. Startup tries new approach to security. Clever ID thieves.

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

- **SecureScout EagleBox SP**

The netVigilance SecureScout EagleBox SP 2.0 is a highly comprehensive vulnerability management product. This tool is customized and tailored to the environment for absolute pinpoint accuracy and in-depth vulnerability analysis. The feature that sets this product apart from others in this space is that the box is designed for multiple users

to manage specific network segments. This provides the ability to segment out a large environment for more specific attention to detail.

We found this product to be quite easy to install in our environment. NetVigilance did some preconfiguration for us as this is part of their customer service process. Once we installed the box in our network, we began setting up targets and scanning our test network.

SC Magazine

Full story : <http://www.scmagazineus.com/SecureScout-EagleBox-SP/Review/2523/>

• 07 Aug 2008 17:33:05 Corporations prepare for start of Olympics

With the start of the Olympics hours away, security experts expect companies to see an increase in bandwidth use, as well as an increase in potential securities risks, as employees watch the sporting events via streaming video.

NBCOlympics.com will be providing more than 2,200 hours of live coverage from Beijing, while other websites will offer highlights. Not only will the website video allow viewers to watch the games in real time, they'll feature events that aren't usually found on television.

However, the ubiquity of streaming radio and video poses significant productivity, bandwidth cost and security challenges for companies of all sizes, according to content filtering firm 8e6 Technologies. One user accessing streaming media can cause up to 20 to 30 percent slowdown in overall network performance, while users accessing blocked websites via anonymous web proxies opens up networks to possible security breaches via bots and other malware.

SC Magazine

Full story: <http://www.scmagazineus.com/Corporations-prepare-for-start-of-Olympics/article/113569/>

05 Aug 2008 13:00:00 Internet security moves to the cloud

August 5, 2008 (Network World) FRAMINGHAM — A start-up that dishes up an in-the-cloud security service says it also eliminates capital outlay for security gear and reduces ongoing support costs.

The service applies policies only to outbound Internet traffic on the fly and can

eliminate the need for multiple single-function devices at the edge of corporate networks, says the company's founder, Jay Chaudhry. He is also the founder of Cipher Trust (now part of Secure Computing), AirDefense (now part of Motorola) and SecureIT (now part of VeriSign).

The Weather Channel has tested the service and may sign up for it within the month, says John Penrod, CISO for the TV network. He says he is being cautious about how the service affects performance as perceived by users, but so far he has seen latency of less than 1 second imposed on traffic filtered by Zscaler.

Computerworld

Full story:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9111535&source=rss_topic17

• 06 Aug 2008 13:00:00 ID theft ring attacked retailers on multiple levels

August 6, 2008 (IDG News Service) A ring of identity thieves that targeted U.S. retailers used sophisticated and multifaceted attacks to steal more than 40 million credit and debit card numbers from TJX, OfficeMax, Barnes & Noble and other companies, according to court documents.

Members of the ID theft conspiracy used so-called war-driving techniques to find holes in wireless networks operated by retail stores. Once inside the networks, the thieves located and stole credit card transaction information stored on the retailers' networks, according to court documents.

The ID theft group stored the captured credit card numbers on compromised servers in the U.S., Latvia and the Ukraine, according to court documents. The thieves then encrypted the credit card numbers on those servers, according to the indictment document of Albert Gonzalez, the alleged ringleader of the ID theft scheme.

Computerworld

Full story:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9111880&source=rss_topic17

New Vulnerabilities Tested in SecureScout

• **16996 Oracle Application Server - Oracle Portal component unspecified Vulnerability (jul-2008/CVE-2008-2589)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Oracle Portal" 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/cpujul2008.html>

* SECUNIA: 31087

<http://secunia.com/advisories/31087/>

* MISC: PLSQL Injection in Oracle Application Server

<http://archives.neohapsis.com/archives/fulldisclosure/2008-07/0240.html>

CVE Reference:

CVE-2008-2589 (cve.mitre.org, nvd.nist.gov)

• **16997 Oracle Application Server - Oracle Portal component unspecified Vulnerability (jul-2008/CVE-2008-2594)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Oracle Portal" 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/cpujul2008.html>

* SECUNIA: 31087

<http://secunia.com/advisories/31087/>

CVE Reference:

CVE-2008-2594 (cve.mitre.org, nvd.nist.gov)

• **16998 Oracle Application Server - Oracle Portal component unspecified Vulnerability (jul-2008/CVE-2008-2609)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Oracle Portal" 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/cpujul2008.html>

* SECUNIA: 31087

<http://secunia.com/advisories/31087/>

CVE Reference:

CVE-2008-2609 (cve.mitre.org, nvd.nist.gov)

• 16999 Oracle Application Server - Oracle Internet Directory component unspecified Vulnerability (jul-2008/CVE-2008-2595)

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

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS** Risk: **Medium**

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html>

* SECUNIA: 31087

<http://secunia.com/advisories/31087/>

* IDEFENSE: Oracle Internet Directory Pre-Authentication LDAP DoS Vulnerability

<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=725>

CVE Reference:

CVE-2008-2595 (cve.mitre.org, nvd.nist.gov)

• 17269 Oracle Application Server - Hyperion BI Plus component unspecified Vulnerability (jul-2008/CVE-2008-2612)

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Hyperion BI Plus" component.

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

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html>

* SECUNIA: 31087

<http://secunia.com/advisories/31087/>

CVE Reference:

CVE-2008-2612 (cve.mitre.org, nvd.nist.gov)

- **18039 Oracle Application Server - Oracle HTTP Server component unspecified Vulnerability (jul-2008/CVE-2008-2614)**

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/cpujul2008.html>

* SECUNIA: 31087

<http://secunia.com/advisories/31087/>

CVE Reference:

CVE-2008-2614 (cve.mitre.org, nvd.nist.gov)

- **18041 Oracle Application Server - Oracle Portal component unspecified Vulnerability (jul-2008/CVE-2008-2593)**

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/cpujul2008.html>

* SECUNIA: 31087

<http://secunia.com/advisories/31087/>

CVE Reference:

CVE-2008-2593 (cve.mitre.org, nvd.nist.gov)

- **18044 RealPlayer (10/10.5/11) ActiveX controls property heap memory corruption (Remote File Checking)**

The WindowName and Controls properties of rmoc3260.dll do not manage heap memory properly resulting in a use after free condition which can overwrite heap management structures resulting in code execution. Note that this is the same issue that affected the Console property(which was fixed in Real Player 11.0.2/rmoc3260.dll version 6.0.10.50, however these were not).

The vulnerability is reported in:

RealPlayer 11 (11.0.0 - 11.0.2 builds 6.0.14.738 - 6.0.14.802
RealPlayer 10.5 (6.0.12.1040-6.0.12.1663, 6.0.12.1698, 6.0.12.1741
RealPlayer 10
RealPlayer Enterprise

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

References:

- * BUGTRAQ: 20080725 ZDI-08-047: RealNetworks RealPlayer rmoc3260 ActiveX Control Memory Corruption Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/494779/100/0/threaded>
- * FULLDISC: 20080310 Real Networks RealPlayer ActiveX Control Heap Corruption
<http://lists.grok.org.uk/pipermail/full-disclosure/2008-March/060659.html>
- * MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-08-047/>
- * CONFIRM:
http://service.real.com/realplayer/security/07252008_player/en/
- * CERT-VN: VU#831457
<http://www.kb.cert.org/vuls/id/831457>
- * BID: 28157
<http://www.securityfocus.com/bid/28157>
- * FRSIRT: ADV-2008-0842
<http://www.frsirt.com/english/advisories/2008/0842>
- * SECTrack: 1019576
<http://www.securitytracker.com/id?1019576>
- * SECUNIA: 29315
<http://secunia.com/advisories/29315>
- * XF: realplayer-realaudioobjects-code-execution(41087)
<http://xforce.iss.net/xforce/xfdb/41087>

CVE Reference:

CVE-2008-1309 (cve.mitre.org, nvd.nist.gov)

• 18045 RealPlayer (10/10.5) Local resource reference vulnerability (Remote File Checking)

Unspecified vulnerability in RealNetworks RealPlayer Enterprise, RealPlayer 10, and RealPlayer 10.5 before build 6.0.12.1675 has unknown impact and attack vectors, probably related to accessing local files, aka a "Local resource reference vulnerability."

The vulnerability is reported in:

RealPlayer 10.5 (6.0.12.1040-6.0.12.1663, 6.0.12.1698, 6.0.12.1741
RealPlayer 10
RealPlayer Enterprise

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Gather Info / Attack** Risk: **High**

References:

* CONFIRM:

http://service.real.com/realplayer/security/07252008_player/en/

* SECUNIA: 27620

<http://secunia.com/advisories/27620/>

CVE Reference:

CVE-2008-3064 (cve.mitre.org, nvd.nist.gov)

• 18048 RealPlayer (10/10.5) SWF file heap-based buffer overflow vulnerability (Remote File Checking)

Heap-based buffer overflow in the Shockwave Flash (SWF) frame handling in RealNetworks RealPlayer 10.5 Build 6.0.12.1483 might allow remote attackers to execute arbitrary code via a crafted SWF file.

The vulnerability is reported in:

RealPlayer 10.5 (6.0.12.1040-6.0.12.1663, 6.0.12.1698, 6.0.12.1741

RealPlayer 10

RealPlayer Enterprise

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

References:

* BUGTRAQ: 20080725 Secunia Research: RealPlayer SWF Frame Handling Buffer Overflow

<http://www.securityfocus.com/archive/1/archive/1/494749/100/0/threaded>

* MISC:

http://secunia.com/secunia_research/2007-93/advisory/

* CONFIRM:

http://service.real.com/realplayer/security/07252008_player/en/

* REDHAT: RHSA-2008:0812

<http://www.redhat.com/support/errata/RHSA-2008-0812.html>

* CERT-VN: VU#298651

<http://www.kb.cert.org/vuls/id/298651>

* SECUNIA: 27620

<http://secunia.com/advisories/27620>

* SECUNIA: 31321

<http://secunia.com/advisories/31321>

CVE Reference:

CVE-2007-5400 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• 16996 Oracle Application Server - Oracle Portal component unspecified Vulnerability (jul-2008/CVE-2008-2589)

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Oracle Portal" 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/cpujul2008.html>

* SECUNIA: 31087

<http://secunia.com/advisories/31087/>

* MISC: PLSQL Injection in Oracle Application Server

<http://archives.neohapsis.com/archives/fulldisclosure/2008-07/0240.html>

CVE Reference:

CVE-2008-2589 (cve.mitre.org, nvd.nist.gov)

• **16997 Oracle Application Server - Oracle Portal component unspecified Vulnerability (jul-2008/CVE-2008-2594)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Oracle Portal" 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/cpujul2008.html>

* SECUNIA: 31087

<http://secunia.com/advisories/31087/>

CVE Reference:

CVE-2008-2594 (cve.mitre.org, nvd.nist.gov)

• **16998 Oracle Application Server - Oracle Portal component unspecified Vulnerability (jul-2008/CVE-2008-2609)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Oracle Portal" 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/cpujul2008.html>

* SECUNIA: 31087
<http://secunia.com/advisories/31087/>

CVE Reference:

CVE-2008-2609 (cve.mitre.org, nvd.nist.gov)

• **16999 Oracle Application Server - Oracle Internet Directory component unspecified Vulnerability (jul-2008/CVE-2008-2595)**

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

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS** Risk: **Medium**

References:

* CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html>
* SECUNIA: 31087
<http://secunia.com/advisories/31087/>
* IDEFENSE: Oracle Internet Directory Pre-Authentication LDAP DoS Vulnerability
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=725>

CVE Reference:

CVE-2008-2595 (cve.mitre.org, nvd.nist.gov)

• **17269 Oracle Application Server - Hyperion BI Plus component unspecified Vulnerability (jul-2008/CVE-2008-2612)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Hyperion BI Plus" component.

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

References:

* CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html>
* SECUNIA: 31087
<http://secunia.com/advisories/31087/>

CVE Reference:

CVE-2008-2612 (cve.mitre.org, nvd.nist.gov)

• **18039 Oracle Application Server - Oracle HTTP Server component unspecified Vulnerability (jul-2008/CVE-2008-2614)**

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/cpujul2008.html>

* SECUNIA: 31087

<http://secunia.com/advisories/31087/>

CVE Reference:

CVE-2008-2614 (cve.mitre.org, nvd.nist.gov)

• 18041 Oracle Application Server - Oracle Portal component unspecified Vulnerability (jul-2008/CVE-2008-2593)

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/cpujul2008.html>

* SECUNIA: 31087

<http://secunia.com/advisories/31087/>

CVE Reference:

CVE-2008-2593 (cve.mitre.org, nvd.nist.gov)

• 18044 RealPlayer (10/10.5/11) ActiveX controls property heap memory corruption (Remote File Checking)

The WindowName and Controls properties of rmoc3260.dll do not manage heap memory properly resulting in a use after free condition which can overwrite heap management structures resulting in code execution. Note that this is the same issue that affected the Console property(which was fixed in Real Player 11.0.2/rmoc3260.dll version 6.0.10.50, however these were not).

The vulnerability is reported in:

RealPlayer 11 (11.0.0 - 11.0.2 builds 6.0.14.738 - 6.0.14.802

RealPlayer 10.5 (6.0.12.1040-6.0.12.1663, 6.0.12.1698, 6.0.12.1741

RealPlayer 10

RealPlayer Enterprise

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

References:

- * BUGTRAQ: 20080725 ZDI-08-047: RealNetworks RealPlayer rmoc3260 ActiveX Control Memory Corruption Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/494779/100/0/threaded>
- * FULLDISC: 20080310 Real Networks RealPlayer ActiveX Control Heap Corruption
<http://lists.grok.org.uk/pipermail/full-disclosure/2008-March/060659.html>
- * MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-08-047/>
- * CONFIRM:
http://service.real.com/realplayer/security/07252008_player/en/
- * CERT-VN: VU#831457
<http://www.kb.cert.org/vuls/id/831457>
- * BID: 28157
<http://www.securityfocus.com/bid/28157>
- * FRSIRT: ADV-2008-0842
<http://www.frsirt.com/english/advisories/2008/0842>
- * SECTrack: 1019576
<http://www.securitytracker.com/id?1019576>
- * SECUNIA: 29315
<http://secunia.com/advisories/29315>
- * XF: realplayer-realaudioobjects-code-execution(41087)
<http://xforce.iss.net/xforce/xfdb/41087>

CVE Reference:

CVE-2008-1309 (cve.mitre.org, nvd.nist.gov)

• 18045 RealPlayer (10/10.5) Local resource reference vulnerability (Remote File Checking)

Unspecified vulnerability in RealNetworks RealPlayer Enterprise, RealPlayer 10, and RealPlayer 10.5 before build 6.0.12.1675 has unknown impact and attack vectors, probably related to accessing local files, aka a "Local resource reference vulnerability."

The vulnerability is reported in:

RealPlayer 10.5 (6.0.12.1040-6.0.12.1663, 6.0.12.1698, 6.0.12.1741)

RealPlayer 10

RealPlayer Enterprise

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Gather Info / Attack** Risk: **High**

References:

- * CONFIRM:
http://service.real.com/realplayer/security/07252008_player/en/
- * SECUNIA: 27620
<http://secunia.com/advisories/27620/>

CVE Reference:

CVE-2008-3064 (cve.mitre.org, nvd.nist.gov)

• **18048 RealPlayer (10/10.5) SWF file heap-based buffer overflow vulnerability (Remote File Checking)**

Heap-based buffer overflow in the Shockwave Flash (SWF) frame handling in RealNetworks RealPlayer 10.5 Build 6.0.12.1483 might allow remote attackers to execute arbitrary code via a crafted SWF file.

The vulnerability is reported in:

RealPlayer 10.5 (6.0.12.1040-6.0.12.1663, 6.0.12.1698, 6.0.12.1741

RealPlayer 10

RealPlayer Enterprise

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

References:

* BUGTRAQ: 20080725 Secunia Research: RealPlayer SWF Frame Handling Buffer Overflow

<http://www.securityfocus.com/archive/1/archive/1/494749/100/0/threaded>

* MISC:

http://secunia.com/secunia_research/2007-93/advisory/

* CONFIRM:

http://service.real.com/realplayer/security/07252008_player/en/

* REDHAT: RHSA-2008:0812

<http://www.redhat.com/support/errata/RHSA-2008-0812.html>

* CERT-VN: VU#298651

<http://www.kb.cert.org/vuls/id/298651>

* SECUNIA: 27620

<http://secunia.com/advisories/27620>

* SECUNIA: 31321

<http://secunia.com/advisories/31321>

CVE Reference:

CVE-2007-5400 (cve.mitre.org, nvd.nist.gov)

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