netVigilance
assurance has arrived

2007 Issue # 37

ScoutNews

The weekly Security update from the makers of SecureScout

September 21, 2007

Table of Contents

Product Focus

Spida Digispid Worm Scanner – The 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

Security veterans call for new malware category. Virtualization requires new approach to security. RFID hysteria. How to protect yourself..

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

❖ Security gurus look for better ways to classify malware

Although malware categorisation systems exist, a new one is necessary because of the focus on economic crime, say security veterans
Two senior security veterans from Trend Micro are trying to get the industry to change how it classifies malicious software.

They argue that today's classification system, which tends to focus on the technical way the software works, neglects a far more important metric that matters more to users: how it tries to steal your money.

"This is my pet bugaboo — the unclear language," said David Perry, global director for education at Trend. "I come from 26 years of technical support, and it irks me that we protect people against things and they don't know what we're protecting them against."

computerworld

Full Story :
http://computerworld.co.nz/news.nsf/scrt/3B225433B5E3F218CC25735D0012F351

❖ Virtual Servers: More or Less Secure?

Virtual servers can be treated just like thin, densely stacked servers. But that misses the point: virtualization frees the server from its physical "body" and gives it flexibility and portability. To take advantage of these traits we have to adopt security measures that also are dynamic and flexible.
Virtualization is quickly being adopted in many different industries. As virtual machines move from testing and development roles into production, security Relevant Products/Services becomes ever more important. Virtual servers are no less secure than regular servers, and may provide additional security by compartmentalizing applications.

However, when companies deploy virtual servers in production they change their operational practices to take advantage of the flexibility of virtualization Relevant Products/Services. Servers are pooled together, provisioned and deployed automatically from a handful of standardized operating system images and moved around dynamically in response to changes in demand or maintenance needs. These operational practices require a new approach to security.

Data Storage Today

Full Story :
http://www.data-storage-today.com/news/Virtual-Servers--More-or-Less-Secure-/story.xhtml?story_id=111008Z6W8JR

❖ Privacy a hot topic as RFID tagging grows in use

Industry needs to explain the value of RFID, advocate says
Privacy concerns over RFID tagging are reaching new heights, with state legislators introducing and increasingly passing new measures to restrict their use, while employers face a barrage of concern from workers over RFID-embedded identity badges.

Those worries were aired by speakers and attendees at RFID World: Boston today, even as some RFID technology defenders worried that they haven't done enough to promote the value of RFID in tracking tainted foods or counterfeit drugs and of reducing the cost of tracking inventory.

To indicate how extreme the national RFID hysteria has become, one speaker said privacy advocate Katherine Albrecht had urged consumers to microwave new underwear to disable a possible RFID tag and thereby prevent someone from tracking your whereabouts.(However, a check of Albrecht's Web site spychips.com, actually urges not putting items in the microwave to disable an RFID tag because it could cause a fire.)

computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9038058&taxonomyId=17&intsrc=kc_top

❖ Security Vulnerabilities To Watch For

Knowing What You're Looking For Always Helps
Protecting your corporate IT assets from would-be attackers is an important job. For many small to medium-sized enterprises, the job frequently falls into the lap of an IT manager with multiple other, equally important jobs. Keeping up with the latest threats and vulnerabilities could be a full-time job, depending on the amount of exposure and the risk associated with an incident.

Identifying potential trouble spots and understanding the associated risks involved is a good first step. So where does a part-time IT security manager go to get the latest and greatest information that's relevant to his situation? Go to the source, meaning start with your security hardware and software vendors.

processor

Full Story :
http://www.processor.com/editorial/article.asp?Article=articles/p2938/30p38/30p38.asp&GUID=DDFE1F34A1A84870BFC430B9F355459D

New Vulnerabilities Tested in SecureScout

❖ 16633 Mozilla Thunderbird error in the handling of the "src" attribute of IMG elements, arbitrary code execution (Remote File Checking)

A vulnerability has been reported in Mozilla Thunderbird, which can be exploited by malicious people to corrupt memory, and possibly execute arbitrary code.

An error in the handling of the "src" attribute of IMG elements loaded in a frame can be exploited to change the attribute to a "javascript:" URI. This allows execution of arbitrary HTML and script code in a user's browser session.

Version 1.5.0.9 addresses the issue.

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

References:

* BUGTRAQ: 20070102 rPSA-2006-0234-2 firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/455728/100/200/threaded
* BUGTRAQ: 20061222 rPSA-2006-0234-1 firefox
http://www.securityfocus.com/archive/1/archive/1/455145/100/0/threaded

* CONFIRM:
http://www.mozilla.org/security/announce/2006/mfsa2006-72.html
* CONFIRM:
https://issues.rpath.com/browse/RPL-883

CVE Reference: CVE-2006-6503

❖ 16632 Mozilla Thunderbird LiveConnect, arbitrary code execution (Remote File Checking)

A vulnerability has been reported in Mozilla Thunderbird, which can be exploited by malicious people to corrupt memory, and possibly execute arbitrary code.

An error in LiveConnect causes an already freed object to be used and may potentially allow execution of arbitrary code.

Version 1.5.0.9 addresses the issue.

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

References:

* BUGTRAQ: 20070102 rPSA-2006-0234-2 firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/455728/100/200/threaded
* BUGTRAQ: 20061222 rPSA-2006-0234-1 firefox
http://www.securityfocus.com/archive/1/archive/1/455145/100/0/threaded
* CONFIRM:
http://www.mozilla.org/security/announce/2006/mfsa2006-71.html
* CONFIRM:
https://issues.rpath.com/browse/RPL-883
* DEBIAN: DSA-1253
http://www.debian.org/security/2007/dsa-1253
* DEBIAN: DSA-1258
http://www.debian.org/security/2007/dsa-1258
* DEBIAN: DSA-1265
http://www.debian.org/security/2007/dsa-1265
* FEDORA: FEDORA-2006-1491
http://fedoranews.org/cms/node/2297
* FEDORA: FEDORA-2007-004
http://fedoranews.org/cms/node/2338

CVE Reference: CVE-2006-6502

❖ 16631 Mozilla Thunderbird "watch()" JavaScript function, arbitrary code execution (Remote File Checking)

A vulnerability has been reported in Mozilla Thunderbird, which can be exploited by malicious people to corrupt memory, and possibly execute arbitrary code.

An unspecified error in the "watch()" JavaScript function can be exploited to execute arbitrary code.

Version 1.5.0.9 addresses the issue.

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

References:

* BUGTRAQ: 20070102 rPSA-2006-0234-2 firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/455728/100/200/threaded
* BUGTRAQ: 20061222 rPSA-2006-0234-1 firefox
http://www.securityfocus.com/archive/1/archive/1/455145/100/0/threaded
* CONFIRM:
http://www.mozilla.org/security/announce/2006/mfsa2006-70.html
* CONFIRM:
https://issues.rpath.com/browse/RPL-883
* DEBIAN: DSA-1253
http://www.debian.org/security/2007/dsa-1253
* DEBIAN: DSA-1258
http://www.debian.org/security/2007/dsa-1258
* DEBIAN: DSA-1265
http://www.debian.org/security/2007/dsa-1265
* FEDORA: FEDORA-2006-1491
http://fedoranews.org/cms/node/2297
* FEDORA: FEDORA-2007-004
http://fedoranews.org/cms/node/2338

CVE Reference: CVE-2006-6501

❖ 16630 Mozilla Thunderbird buffer overflow when using the CSS cursor property (Remote File Checking)

A vulnerability has been reported in Mozilla Thunderbird, which can be exploited by malicious people to corrupt memory, and possibly execute arbitrary code.

A boundary error when setting the cursor to a Windows bitmap using the CSS cursor property can be exploited to cause a heap-based buffer overflow.

Version 1.5.0.9 addresses the issue.

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

References:

* CONFIRM:
http://www.mozilla.org/security/announce/2006/mfsa2006-69.html
* GENTOO: GLSA-200701-02
http://security.gentoo.org/glsa/glsa-200701-02.xml
* GENTOO: GLSA-200701-03
http://www.gentoo.org/security/en/glsa/glsa-200701-03.xml

* GENTOO: GLSA-200701-04
http://www.gentoo.org/security/en/glsa/glsa-200701-04.xml
* MANDRIVA: MDKSA-2007:010
http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:010
* MANDRIVA: MDKSA-2007:011
http://frontal2.mandriva.com/security/advisories?name=MDKSA-2007:011
* SUSE: SUSE-SA:2006:080
http://www.novell.com/linux/security/advisories/2006_80_mozilla.html
* SUSE: SUSE-SA:2007:006
http://www.novell.com/linux/security/advisories/2007_06_mozilla.html
* CERT: TA06-354A
http://www.us-cert.gov/cas/techalerts/TA06-354A.html

CVE Reference: CVE-2006-6500

❖ 16629 Mozilla Thunderbird memory corruption errors in js_dtoa() (Remote File Checking)

An error when reducing the CPU's floating point precision, which may happen on Windows when loading a plugin creating a Direct3D device, may cause the "js_dtoa()" function to not exit and instead cause a memory corruption.

Version 1.5.0.9 addresses the issue.

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

References:

* CONFIRM:
http://www.mozilla.org/security/announce/2006/mfsa2006-68.html
* DEBIAN: DSA-1253
http://www.debian.org/security/2007/dsa-1253
* DEBIAN: DSA-1258
http://www.debian.org/security/2007/dsa-1258
* DEBIAN: DSA-1265
http://www.debian.org/security/2007/dsa-1265
* GENTOO: GLSA-200701-02
http://security.gentoo.org/glsa/glsa-200701-02.xml
* GENTOO: GLSA-200701-04
http://www.gentoo.org/security/en/glsa/glsa-200701-04.xml
* SUNALERT: 102846
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102846-1
* SUSE: SUSE-SA:2006:080
http://www.novell.com/linux/security/advisories/2006_80_mozilla.html
* SUSE: SUSE-SA:2007:006
http://www.novell.com/linux/security/advisories/2007_06_mozilla.html

CVE Reference: CVE-2006-6499

❖ 16628 Mozilla Thunderbird memory corruption errors in layout engine

and JavaScript engine (Remote File Checking)

A vulnerability has been reported in Mozilla Thunderbird, which can be exploited by malicious people to corrupt memory, and possibly execute arbitrary code.

Various errors in the layout engine and JavaScript engine can be exploited to cause memory corruption and some may potentially allow execution of arbitrary code.

Version 1.5.0.9 addresses the issue.

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

References:

* BUGTRAQ: 20070102 rPSA-2006-0234-2 firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/455728/100/200/threaded
* BUGTRAQ: 20061222 rPSA-2006-0234-1 firefox
http://www.securityfocus.com/archive/1/archive/1/455145/100/0/threaded
* CONFIRM:
http://www.mozilla.org/security/announce/2006/mfsa2006-68.html
* CONFIRM:
https://issues.rpath.com/browse/RPL-883
* DEBIAN: DSA-1253
http://www.debian.org/security/2007/dsa-1253
* DEBIAN: DSA-1258
http://www.debian.org/security/2007/dsa-1258
* DEBIAN: DSA-1265
http://www.debian.org/security/2007/dsa-1265

CVE Reference: CVE-2006-6498

❖ 16627 Mozilla Thunderbird layout engine, JavaScript engine, and in SVG, multiple memory corruption errors Vulnerability (Remote File Checking)

Some vulnerabilities have been reported in Mozilla Thunderbird, which can be exploited by malicious people to execute arbitrary code on a user's system.

Multiple memory corruption errors exist in the layout engine, JavaScript engine, and in SVG. Some of these may be exploited to execute arbitrary code on a user's system.

The weakness is confirmed in version prior to 1.5.0.10.

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

References:

* BUGTRAQ: 20070226 rPSA-2007-0040-1 firefox
http://www.securityfocus.com/archive/1/archive/1/461336/100/0/threaded
* BUGTRAQ: 20070303 rPSA-2007-0040-3 firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/461809/100/0/threaded
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-01.html

* CONFIRM:
https://issues.rpath.com/browse/RPL-1081
* CONFIRM:
https://issues.rpath.com/browse/RPL-1103
* DEBIAN: DSA-1336
http://www.debian.org/security/2007/dsa-1336
* FEDORA: FEDORA-2007-281
http://fedoranews.org/cms/node/2713
* FEDORA: FEDORA-2007-293
http://fedoranews.org/cms/node/2728

CVE Reference: CVE-2007-0775

❖ 16626 Mozilla Thunderbird Network Security Services, integer underflow Vulnerability (Remote File Checking)

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

An integer underflow error in the Network Security Services (NSS) code when processing SSLv2 server messages can be exploited to cause a heap-based buffer overflow via a certificate with a public key too small to encrypt the "Master Secret".

Successful exploitation may allow execution of arbitrary code.

The weakness is confirmed in versions 1.5 before 1.5.0.10.

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

References:

* BUGTRAQ: 20070226 rPSA-2007-0040-1 firefox
http://www.securityfocus.com/archive/1/archive/1/461336/100/0/threaded
* BUGTRAQ: 20070303 rPSA-2007-0040-3 firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/461809/100/0/threaded
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-06.html
* IDEFENSE: 20070223 Mozilla Network Security Services SSLv2 Client Integer Underflow Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=482
* MISC:
https://bugzilla.mozilla.org/show_bug.cgi?id=364319
* CONFIRM:
https://issues.rpath.com/browse/RPL-1081
* CONFIRM:
https://issues.rpath.com/browse/RPL-1103
* DEBIAN: DSA-1336
http://www.debian.org/security/2007/dsa-1336
* FEDORA: FEDORA-2007-278
http://fedoranews.org/cms/node/2709

CVE Reference: CVE-2007-0008

❖ 16625 Mozilla Thunderbird - Javascript engine memory corruption, arbitrary code execution and denial of service Vulnerabilities (Remote File Checking)

Multiple unspecified vulnerabilities in the JavaScript engine in Mozilla Firefox before 2.0.0.5 and Thunderbird before 2.0.0.5 allow remote attackers to cause a denial of service (crash) via unspecified vectors that trigger memory corruption.

The issue has been fixed in Thunderbird 2.0.0.5.

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

References:

* BUGTRAQ: 20070720 rPSA-2007-0148-1 firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/474226/100/0/threaded
* BUGTRAQ: 20070724 FLEA-2007-0033-1: firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/474542/100/0/threaded
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-18.html
* CONFIRM:
ftp://ftp.slackware.com/pub/slackware/slackware-12.0/ChangeLog.txt
* CONFIRM:
http://support.novell.com/techcenter/psdb/07d098f99c9fe6956523beae37f32fda
.html
* DEBIAN: DSA-1337
http://www.debian.org/security/2007/dsa-1337

CVE Reference: CVE-2007-3735

❖ 16624 Mozilla Thunderbird - Memory corruption, arbitrary code execution and denial of service Vulnerabilities (Remote File Checking)

Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 2.0.0.5 and Thunderbird before 2.0.0.5 allow remote attackers to cause a denial of service (crash) via unspecified vectors that trigger memory corruption.

The issue has been fixed in Thunderbird 2.0.0.5.

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

References:

* BUGTRAQ: 20070720 rPSA-2007-0148-1 firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/474226/100/0/threaded
* BUGTRAQ: 20070724 FLEA-2007-0033-1: firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/474542/100/0/threaded
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-18.html
* CONFIRM:

ftp://ftp.slackware.com/pub/slackware/slackware-12.0/ChangeLog.txt
* CONFIRM:
http://support.novell.com/techcenter/psdb/07d098f99c9fe6956523beae37f32fda.html
* DEBIAN: DSA-1337
http://www.debian.org/security/2007/dsa-1337

CVE Reference: CVE-2007-3734

New Vulnerabilities found this Week

VMware ESX Server Multiple Security Updates

"Bypass security restrictions; Gain escalated privileges; Denial of Service"

VMware has issued an update for VMware ESX Server. This fixes some vulnerabilities, which can be exploited by malicious, local users to bypass certain security restrictions, perform certain actions with escalated privileges, or to cause a DoS (Denial of Service), by malicious users to bypass certain security restrictions, and by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

References:
http://lists.grok.org.uk/pipermail/full-disclosure/2007-September/065902.html

Firefox "-chrome" Parameter Security Issue

"Execution of arbitrary Javascript script"

Mozilla has acknowledged a security issue in Firefox, which potentially can be exploited by malicious people to compromise a user's system.

The security issue is caused due to the "-chrome" parameter allowing execution of arbitrary Javascript script code in chrome context. This can be exploited to execute arbitrary commands on a user's system e.g. via applications invoking Firefox with unfiltered command line arguments.

References:
http://www.mozilla.org/security/announce/2007/mfsa2007-28.html

AOL Instant Messenger Notification Window Script Execution Vulnerability

"Execute arbitrary script code"

Shell has discovered a vulnerability in AOL Instant Messenger, which can be exploited by malicious people to execute arbitrary script code.

Input passed to the Notification window is not properly sanitized before being displayed to the user. This can be exploited to execute a limited amount of arbitrary script code in the Local Zone (My Computer) context by e.g. sending a specially crafted message to another user.

Successful exploitation requires that the target user is e.g. chatting with a different user so that the Notification window is shown and that the attacker is in the Buddy List of the target user or the target user accepts the IM message from the attacker.

The vulnerability is confirmed in version 6.1.41.2. Other versions may also be affected.

References:
http://secunia.com/advisories/26786/

OpenOffice TIFF Parsing Integer Overflow Vulnerabilities

"Execution of arbitrary code"

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

The vulnerabilities are caused due to integer overflows when processing certain tags within TIFF images. This can be exploited to cause heap-based buffer overflows by e.g. tricking a user into opening a specially crafted document.

Successful exploitation may allow the execution of arbitrary code.

The vulnerabilities are reported in versions prior to 2.3.

References:
http://www.openoffice.org/security/cves/CVE-2007-2834.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