netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 2

January 12, 2007

Table of Contents

Product Focus

Sapphire Worm Scanner – The Sapphire 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 Microsoft SQL buffer overflow vulnerability (MS02-039/MS02-061) that the recent Sapphire Worm uses to propagate.

netVigilance, Inc is proud to announce that we have been awarded the Payment Card Industry (PCI) Certifications as "Approved Scanning Vendor" (ASV).
This Certification allows netVigilance, Inc to determine PCI Data Security Standard (DSS) Compliance for vendors accepting Credit Cards on a worldwide basis.

This Week in Review

What to do when vendors won't patch? Corporate data leakage a big issue. Mobile malware on the rise, security services too. Crooks have started using code obfuscation.

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

- **Customers lose when vendors refuse to patch**

I can't believe my eyes. Eudora WorldMail Mail Management Server has an open

exploit hole and Qualcomm says they have no plans to patch.
Tipping Point and the Zero Point Initiative reported last week that Eudora WorldMail 3.1.x Mail Management Server has a remote exploit accessible over TCP port 106. As the report states, "This vulnerability allows attackers to execute arbitrary code on vulnerable installations of Eudora WorldMail. Authentication is not required to exploit this vulnerability. The specific flaw exists during the parsing of successive delimiters within the Mail Management Server, MAILMA.EXE."

According the report, Qualcomm has no plans to patch this hole. Instead, the vendor apparently encourages end users to use alternate defense-in-depth techniques and block TCP port 106 access from unauthorized computers to affected servers at the network layer.

I had a "You've got to be kidding me!" moment when I read this. The company's response to the exploit hole is unfortunate for Qualcomm's past, existing, and future customers.

Essentially, Qualcomm is saying that it is leaving its customers open to malicious exploitation on purpose, hoping that additional layers of defense-in-depth security will protect them instead.

InfoWorld

Full Story :
http://www.infoworld.com/article/07/01/12/03OPsecadvise_1.html?source=rss&url=http://www.infoworld.com/article/07/01/12/03OPsecadvise_1.html

- **2007 as year of corporate data leakage concerns and growth of profit-driven spam**

Tumbleweed announced the five most pressing messaging security threats that will emerge or continue to plague IT security in 2007. As anticipated, data leakage concerns and continued growth of profit-driven spam will top the list in the coming year.

1. Sensitive data leakage for public companies becomes a huge issue in 2007. Organizations will have to address the fact that sensitive data like intellectual property or customer information is traveling outside the enterprise, typically via unsecured methods.

2. Spam problems will continue to grow and be increasingly profit-driven. Most spam will be focused on a few categories with the most profit potential. For example, 60 percent of spam at end of 2006 was for stock tips or drugs – both areas where there is a clear profit motive and will continue to grow in 2007.

3. Spammers will continue to adapt to exploit new ways to circumvent spam filters. For example, spammers will seek to randomize images to evade spam filters to penetrate inboxes. The most recent example, that will gain more steam in 2007, is "logo gibberish" spam – legitimate graphics thrown into an email to confuse spam filters.

Help Net Security

Full Story :
http://www.net-security.org/secworld.php?id=4604

❖ Mobile Security Services Against Malware

Due to the fact that the shipment as well as use of smartphones is constantly increasing, mobile phones are now much more attractive targets for hackers. Up until smartphones became popular, malware targeting mobile phones was nonexistent. This just proves that the more advanced mobile phones become, it will also be more difficult to provide mobile security. Now, according to ABI Research, the newest and most intriguing market opportunity for mobile security is the growth of mobile device security managed devices.

"There have been close to thirty different types of attack on mobile devices within the past two years", vice president and networking research director
Stan Schatt says. According to him, the mobile device security managed services market will increase in size from around $100 million in 2006 to well over $500 million in 2011.
"While Sprint is now the sole U.S. mobile operator offering such a security service," says Schatt, "we believe others will join in shortly, just as they have in Europe."

Softpedia

Full Story :
http://news.softpedia.com/news/Mobile-Security-Services-Against-Malware-44271.shtml

❖ Cyber-crooks switch to code obfuscation

Security firm Finjan has reported that dynamic code obfuscation was increasingly used as a method to bypass traditional signature-based security systems and propagate malware during the fourth quarter of 2006.

The technique works by providing each visitor to a malicious site with a different instance of obfuscated malicious code, based on random functions and parameter name changes.

A conventional signature-based security solution would theoretically need millions of signatures to detect and block this particular piece of malicious code.

"Dynamic code obfuscation techniques are the latest salvo from hackers in the ongoing battle of wits between security vendors and their hacker opponents," said Yuval Ben-Itzhak, chief technology officer at Finjan.

vnunet

Full Story :
http://www.vnunet.com/vnunet/news/2172438/cyber-crooks-switch-code

New Vulnerabilities Tested in SecureScout

❖ 14487 Adobe Reader Unspecified Heap Corruption Vulnerability (Remote File Checking)

Piotr Bania has reported a vulnerability in Adobe Reader, which can potentially be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an unspecified error when processing PDF files. This can be exploited to cause a heap corruption and may allow execution of arbitrary code when a specially-crafted PDF file is opened.

The vulnerability is reported in version 7.0.8 and prior. Other versions may also be affected.

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

References:

Original advisories:
http://www.piotrbania.com/all/adv/adobe-acrobat-adv.txt

Other references:
http://www.adobe.com/support/security/bulletins/apsb07-01.html

Product HomePage:
http://www.adobe.com/products/

CVE Reference: CVE-2006-5857

❖ 14488 Adobe Reader LoadFile method, Denial of Service and Code execution Vulnerability (Remote File Checking)

Adobe Reader (Adobe Acrobat Reader) 7.0 through 7.0.8 allows remote attackers to cause a denial of service and possibly execute arbitrary code via a long argument string to the LoadFile method in an AcroPDF ActiveX control.

The vulnerability is reported in version 7.0 through 7.0.8. Other versions may also be affected.

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

References:

Original advisories:
http://www.adobe.com/support/security/bulletins/apsb06-20.html

Other references:
BUGTRAQ:20061205 eEye's Zero-Day Tracker Launch
#
URL:http://www.securityfocus.com/archive/1/archive/1/453579/100/0/threaded
MISC: http://downloads.securityfocus.com/vulnerabilities/exploits/21155-AcroPDF_DoS.html
MISC: http://research.eeye.com/html/alerts/zeroday/20061128.html
CERT-VN:VU#198908
URL:http://www.kb.cert.org/vuls/id/198908
BID:21155
URL:http://www.securityfocus.com/bid/21155
FRSIRT:ADV-2006-4751
URL:http://www.frsirt.com/english/advisories/2006/4751
SECTRACK:1017297

URL:http://securitytracker.com/id?1017297
SECUNIA:23138
URL:http://secunia.com/advisories/23138
XF:adobe-acrobat-acropdf-code-execution(30574)
URL:http://xforce.iss.net/xforce/xfdb/30574

Product HomePage:
http://www.adobe.com/products/

CVE Reference: CVE-2006-6027

❖ **14489 Adobe Reader src, setPageMode, setLayoutMode, setNamedDest methods, Denial of Service and Code execution Vulnerability (Remote File Checking)**

Adobe Reader (Adobe Acrobat Reader) 7.0 through 7.0.8 allows remote attackers to cause a denial of service and possibly execute arbitrary code via a long argument string to the (1) src, (2) setPageMode, (3) setLayoutMode, and (4) setNamedDest methods in an AcroPDF ActiveX control, a different set of vectors than CVE-2006-6027.

The vulnerability is reported in version 7.0 through 7.0.8. Other versions may also be affected.

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

References:

Original advisories:
http://www.adobe.com/support/security/bulletins/apsb06-20.html

Other references:
BUGTRAQ:20061205 eEye's Zero-Day Tracker Launch
#
URL:http://www.securityfocus.com/archive/1/archive/1/453579/100/0/threaded
MISC: http://research.eeye.com/html/alerts/zeroday/20061128.html
MISC: http://www.milw0rm.com/exploits/3040
CERT-VN:VU#198908
URL:http://www.kb.cert.org/vuls/id/198908
BID:21338
URL:http://www.securityfocus.com/bid/21338
BID:21813
URL:http://www.securityfocus.com/bid/21813
FRSIRT:ADV-2006-4751
URL:http://www.frsirt.com/english/advisories/2006/475 1
SECUNIA:23138
URL:http://secunia.com/advisories/23138
XF:adobe-acrobat-acropdf-code-execution(30574)
URL:http://xforce.iss.net/xforce/xfdb/30574
XF:adobe-acropdf-activex-dos(31167)
URL:http://xforce.iss.net/xforce/xfdb/31167

Product HomePage:

http://www.adobe.com/products/

CVE Reference: CVE-2006-6236

❖ 16391 Wireshark SSCOP dissector Denial of Service Vulnerability (Remote File Checking)

The SSCOP dissector in Wireshark (formerly Ethereal) before 0.99.3 allows remote attackers to cause a denial of service (resource consumption) via malformed packets that cause the Q.2391 dissector to use excessive memory.

The vulnerabilities have been reported in versions before 0.99.3.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00024.html

Other references:
CONFIRM: http://www.wireshark.org/security/wnpa-sec-2006-02.html
CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-227.htm
DEBIAN:DSA-1171
URL:http://www.debian.org/security/2006/dsa-1171
GENTOO:GLSA-200608-26
URL:http://security.gentoo.org/glsa/glsa-200608-26.xml
MANDRIVA:MDKSA-2006:152
URL:http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:152
REDHAT:RHSA-2006:0658
URL:http://www.redhat.com/support/errata/RHSA-2006-0658.html
CERT-VN:VU#696896
URL:http://www.kb.cert.org/vuls/id/696896
BID:19690
URL:http://www.securityfocus.com/bid/19690
FRSIRT:ADV-2006-3370
URL:http://www.frsirt.com/english/advisories/2006/3370
SECTRACK:1016736
URL:http://securitytracker.com/id?1016736
SECUNIA:21597
URL:http://secunia.com/advisories/21597
SECUNIA:21649
URL:http://secunia.com/advisories/21649
SECUNIA:21813
URL:http://secunia.com/advisories/21813
SECUNIA:21619
URL:http://secunia.com/advisories/21619
SECUNIA:21682
URL:http://secunia.com/advisories/21682
SECUNIA:21885
URL:http://secunia.com/advisories/21885
SECUNIA:22378
URL:http://secunia.com/advisories/22378

XF:wireshark-sscop-dos(28556)
URL:http://xforce.iss.net/xforce/xfdb/28556
XF:wireshark-esp-offbyone(28553)
URL:http://xforce.iss.net/xforce/xfdb/28553

Product Homepage:
http://www.wireshark.org/

CVE Reference: CVE-2006-4333

❖ 16392 Wireshark MIME Multipart dissector Denial of Service Vulnerability (Remote File Checking)

Off-by-one error in the MIME Multipart dissector in Wireshark (formerly Ethereal) 0.10.1 through 0.99.3 allows remote attackers to cause a denial of service (crash) via certain vectors that tragger an assertion error related to unexpected length values.

The vulnerabilities have been reported in versions 0.10.1 through 0.99.3.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00024.html

Other references:
CONFIRM: http://www.wireshark.org/security/wnpa-sec-2006-03.html
CONFIRM: https://issues.rpath.com/browse/RPL-746
CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-255.htm
DEBIAN:DSA-1201
URL:http://www.us.debian.org/security/2006/dsa-1201
MANDRIVA:MDKSA-2006:195
URL:http://www.mandriva.com/security/advisories?name=MDKSA-2006:195
REDHAT:RHSA-2006:0726
URL:http://www.redhat.com/support/errata/RHSA-2006-0726.html
SGI:20061101-01-P
URL:ftp://patches.sgi.com/support/free/security/advisories/20061101-01-P
SUSE:SUSE-SA:2006:065
URL:http://www.novell.com/linux/security/advisories/2006_65_ethereal.html
BID:20762
URL:http://www.securityfocus.com/bid/20762
FRSIRT:ADV-2006-4220
URL:http://www.frsirt.com/english/advisories/2006/4220
SECTRACK:1017129
URL:http://securitytracker.com/id?1017129
SECUNIA:22590
URL:http://secunia.com/advisories/22590
SECUNIA:22692
URL:http://secunia.com/advisories/22692
SECUNIA:22659
URL:http://secunia.com/advisories/22659
SECUNIA:22672

URL:http://secunia.com/advisories/22672
SECUNIA:22797
URL:http://secunia.com/advisories/22797
SECUNIA:22841
URL:http://secunia.com/advisories/22841
SECUNIA:22929
URL:http://secunia.com/advisories/22929
SECUNIA:23096
URL:http://secunia.com/advisories/23096
XF:wireshark-mime-dos(29844)
URL:http://xforce.iss.net/xforce/xfdb/29844

Product Homepage:
http://www.wireshark.org/

CVE Reference: CVE-2006-4574

❖ 16393 Wireshark XOT dissector Denial of Service Vulnerability (Remote File Checking)

epan/dissectors/packet-xot.c in the XOT dissector (dissect_xot_pdu) in Wireshark (formerly Ethereal) 0.9.8 through 0.99.3 allows remote attackers to cause a denial of service (memory consumption and crash) via an encoded XOT packet that produces a zero length value when it is decoded.

The vulnerabilities have been reported in versions 0.9.8 through 0.99.3.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00024.html

Other references:
CONFIRM: http://www.wireshark.org/security/wnpa-sec-2006-03.html
CONFIRM: https://issues.rpath.com/browse/RPL-746
CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-255.htm
DEBIAN:DSA-1201
URL:http://www.us.debian.org/security/2006/dsa-1201
MANDRIVA:MDKSA-2006:195
URL:http://www.mandriva.com/security/advisories?name=MDKSA-2006:195
REDHAT:RHSA-2006:0726
URL:http://www.redhat.com/support/errata/RHSA-2006-0726.html
SGI:20061101-01-P
URL:ftp://patches.sgi.com/support/free/security/advisories/20061101-01-P
SUSE:SUSE-SA:2006:065
URL:http://www.novell.com/linux/security/advisories/2006_65_ethereal.html
CERT-VN:VU#723736
URL:http://www.kb.cert.org/vuls/id/723736
BID:20762
URL:http://www.securityfocus.com/bid/20762
FRSIRT:ADV-2006-4220

URL:http://www.frsirt.com/english/advisories/2006/4220
SECTRACK:1017129
URL:http://securitytracker.com/id?1017129
SECUNIA:22590
URL:http://secunia.com/advisories/22590
SECUNIA:22692
URL:http://secunia.com/advisories/22692
SECUNIA:22659
URL:http://secunia.com/advisories/22659
SECUNIA:22672
URL:http://secunia.com/advisories/22672
SECUNIA:22797
URL:http://secunia.com/advisories/22797
SECUNIA:22841
URL:http://secunia.com/advisories/22841
SECUNIA:22929
URL:http://secunia.com/advisories/22929
SECUNIA:23096
URL:http://secunia.com/advisories/23096
XF:wireshark-xot-dos(29843)
URL:http://xforce.iss.net/xforce/xfdb/29843

Product Homepage:
http://www.wireshark.org/

CVE Reference: CVE-2006-4805

❖ 16394 Wireshark WBXML dissector Denial of Service Vulnerability (Remote File Checking)

Unspecified vulnerability in the WBXML dissector in Wireshark (formerly Ethereal) 0.10.11 through 0.99.3 allows remote attackers to cause a denial of service (crash) via certain vectors that trigger a null dereference.

The vulnerabilities have been reported in versions 0.10.11 through 0.99.3.

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

References:

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00024.html

Other references:
CONFIRM: http://www.wireshark.org/security/wnpa-sec-2006-03.html
CONFIRM: https://issues.rpath.com/browse/RPL-746
CONFIRM: http://support.avaya.com/elmodocs2/security/ASA-2006-255.htm
MANDRIVA:MDKSA-2006:195
URL:http://www.mandriva.com/security/advisories?name=MDKSA-2006:195
REDHAT:RHSA-2006:0726
URL:http://www.redhat.com/support/errata/RHSA-2006-0726.html
SGI:20061101-01-P
URL:ftp://patches.sgi.com/support/free/security/advisories/20061101-01-P

SUSE:SUSE-SA:2006:065
URL:http://www.novell.com/linux/security/advisories/2006_65_ethereal.html
BID:20762
URL:http://www.securityfocus.com/bid/20762
FRSIRT:ADV-2006-4220
URL:http://www.frsirt.com/english/advisories/2006/4220
SECTRACK:1017129
URL:http://securitytracker.com/id?1017129
SECUNIA:22590
URL:http://secunia.com/advisories/22590
SECUNIA:22692
URL:http://secunia.com/advisories/22692
SECUNIA:22672
URL:http://secunia.com/advisories/22672
SECUNIA:22797
URL:http://secunia.com/advisories/22797
SECUNIA:22841
URL:http://secunia.com/advisories/22841
SECUNIA:22929
URL:http://secunia.com/advisories/22929
SECUNIA:23096
URL:http://secunia.com/advisories/23096
XF:wireshark-wbxml-dos(29842)
URL:http://xforce.iss.net/xforce/xfdb/29842

Product Homepage:
http://www.wireshark.org/

CVE Reference: CVE-2006-5469

❖ 16395 Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (MS07-002/927198) (Remote File Checking)

Excel Malformed IMDATA Record Vulnerability - CVE-2007-0027:

A remote code execution vulnerability exists in Microsoft Excel. An attacker could exploit this vulnerability when Excel parses a file and processes a malformed IMDATA record.

Excel Malformed Record Vulnerability - CVE-2007-0028:

A remote code execution vulnerability exists in Microsoft Excel. An attacker could exploit this vulnerability when Excel parses a file and processes a malformed record.

Excel Malformed String Vulnerability - CVE-2007-0029:

A remote code execution vulnerability exists in Microsoft Excel that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

Excel Malformed Column Record Vulnerability - CVE-2007-0030:

A remote code execution vulnerability exists in Microsoft Excel. An attacker could exploit this vulnerability when Excel parses a file and processes a malformed Column

record.

Excel Malformed Palette Record Vulnerability - CVE-2007-0031:

A remote code execution vulnerability exists in Microsoft Excel. An attacker could exploit this vulnerability when Excel parses a file and processes a malformed Palette record.

If a user were logged on with administrative user rights, an attacker who successfully exploited one of these vulnerabilities could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

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

References:

Original advisory:
MS07-002
http://www.microsoft.com/technet/security/Bulletin/MS07-002.mspx

Other references:
* IDEFENSE:20070109 Microsoft Excel Long Palette Heap Overflow Vulnerability
* URL:http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=461

CVE Reference: CVE-2007-0027
CVE-2007-0028
CVE-2007-0029
CVE-2007-0030
CVE-2007-0031

❖ 16396 Vulnerabilities in Microsoft Outlook Could Allow Remote Code Execution (MS07-003/925938) (Remote File Checking)

Microsoft Outlook VEVENT Vulnerability - CVE-2007-0033:

A remote code execution vulnerability exists in Microsoft Outlook. An attacker could exploit this vulnerability when Outlook parses a file and processes a malformed VEVENT record.

Microsoft Outlook Denial of Service Vulnerability – CVE-2006-1305:

A denial of service vulnerability exists in Outlook in its processing of e-mail header information. An attacker who successfully exploited the vulnerability could send a malformed e-mail to a user of Outlook that would cause the Outlook client to fail under certain circumstances. The Outlook client would continue to fail so long as the malformed e-mail message remained on the e-mail server. The e-mail message could be deleted by an e-mail administrator, or by the user via another e-mail client such as Outlook Web Access or Outlook Express, after which point the Outlook client would again function normally.

Microsoft Outlook Advanced Find Vulnerability - CVE-2007-0034:

A remote code execution vulnerability exists in Microsoft Outlook. An attacker could exploit this vulnerability when Outlook parses an .oss file.

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

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

References:

Original advisory:
MS07-003
http://www.microsoft.com/technet/security/Bulletin/MS07-003.mspx

CVE Reference: CVE-2007-0033
CVE-2006-1305
CVE-2007-0034

❖ **16397 Vulnerability in Vector Markup Language Could Allow Remote Code Execution (MS07-004/929969) (Remote File Checking)**

A remote code execution vulnerability exists in the Vector Markup Language (VML) implementation in Microsoft Windows. An attacker could exploit the vulnerability by constructing a specially crafted Web page or HTML e-mail that could potentially allow remote code execution if a user visited the Web page or viewed the message. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

Original advisory:
MS07-004
http://www.microsoft.com/technet/security/Bulletin/MS07-004.mspx

Other references:
* IDEFENSE:20070109 Microsoft Windows VML Element Integer Overflow Vulnerability
* URL:http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=462

CVE Reference: CVE-2007-0024

New Vulnerabilities found this Week

Microsoft Windows Vector Markup Language Buffer Overflow

“Execution of arbitrary code”

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

The vulnerability is caused due to an integer overflow error in the Vector Markup Language (VML) implementation and can be exploited to cause a heap-based buffer overflow via e.g. a specially crafted web page or HTML e-mail.

Successful exploitation allows execution of arbitrary code.

NOTE: According to Microsoft, the vulnerability is being actively exploited.

References:
http://www.microsoft.com/technet/security/Bulletin/MS07-004.mspx
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=462
http://www.kb.cert.org/vuls/id/122084

Apple Mac OS X UFS ffs_mountfs() Integer Overflow

“Execution of arbitrary code”

LMH has reported a vulnerability in Mac OS X, which can potentially be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an integer overflow error in the "ffs_mountfs()" function when handling UFS file system disc images. This can be exploited to cause a heap-based buffer overflow via a specially crafted UFS DMG image.

Successful exploitation may allow the execution of arbitrary code.

NOTE: This is only remotely exploitable via the Safari web browser when the "opening safe files after downloading" option is enabled.

The vulnerability is reported in an updated Mac OS X 10.4.8. Other versions may also be affected.

References:
http://projects.info-pull.com/moab/MOAB-10-01-2007.html

Adobe Reader Unspecified Heap Corruption Vulnerability

“Execution of arbitrary cod”

Piotr Bania has reported a vulnerability in Adobe Reader, which can potentially be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an unspecified error when processing PDF files. This can be exploited to cause a heap corruption and may allow execution of arbitrary code when a specially-crafted PDF file is opened.

The vulnerability is reported in version 7.0.8 and prior. Other versions may also be affected.

References:

http://www.piotrbania.com/all/adv/adobe-acrobat-adv.txt
http://www.adobe.com/support/security/bulletins/apsb07-01.html

Linux Kernel Local Denial of Service Vulnerabilities

"Denial of Service"

Some vulnerabilities have been reported in the Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

1) An error exists within the handling of locking semaphores in "mincore()". This can be exploited to cause a deadlock by using the function on unmapped pages.

2) An error exists within the "zlib_inflate()" function when processing certain data streams. This can be exploited to corrupt memory by e.g. mounting a specially crafted cramfs image and performing a read operation on the mounted file system.

3) The Kernel fails to handle corrupted data structures in the Ext2 file system correctly. This can be exploited to crash the system by mounting and reading a specially crafted file system image.

The vulnerabilities are reported in versions prior to 2.6.19.2.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.19.2

phpMyAdmin Cross-Site Scripting and Unspecified Vulnerabilities

"Cross-site scripting attacks"

ome vulnerabilities have been reported in phpMyAdmin, some of which have unknown impacts, while some can be exploited by malicious people to conduct cross-site scripting attacks.

1) Input passed to unspecified parameters is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

2) Some vulnerabilities exist, which are caused due to unspecified errors in phpMyAdmin. No further information is currently available.

The vulnerabilities are reported in version 2.9.1.1. Other versions may also be affected.

References:
http://www.phpmyadmin.net/home_page/downloads.php?relnotes=0

Sun Solaris rpcbind Denial of Service

"Denial of Service"

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

The vulnerability is caused due to an unspecified error in libnsl when handling malformed

RPC requests, and can be exploited to kill the rpcbind server.

The vulnerability is reported in Sun Solaris 8 and 9 for the SPARC and x86 platforms.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102713-1

VMWare ESX Server Multiple Vulnerabilities

"Gain knowledge of sensitive information; bypass security restrictions; Denial of Service; Gain escalated privileges"

Some vulnerabilities have been reported in VMWare ESX Server, which can be exploited by malicious people to gain knowledge of sensitive information, bypass certain security restrictions, cause a DoS (Denial of Service), gain escalated privileges, or compromise a system.

References:
http://www.vmware.com/support/vi3/doc/esx-9986131-patch.html
http://www.vmware.com/support/vi3/doc/esx-3069097-patch.html
http://www.vmware.com/support/esx25/doc/esx-254-200612-patch.html
http://www.vmware.com/support/esx25/doc/esx-253-200612-patch.html
http://www.vmware.com/support/esx21/doc/esx-213-200612-patch.html
http://www.vmware.com/support/esx2/doc/esx-202-200612-patch.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