netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 28

July 14, 2006

Table of Contents

Product Focus

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.

This Week in Review

Companies starting to look into mobile security. EU working on RFID security. E-mail surpassed by websites as #1 for virus spreading.

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

- **Don't Spring a Data Leak**

One of the CIO's nightmares du jour: A laptop with sensitive info gets lost or stolen, landing the organization in the headlines. Here's how enterprises are stepping up their safeguards.

Steven Zimmerman, vice president of technology risk management for Regions Financial Corp., a financial services company in Birmingham, Ala., with $85 billion in assets, used to get challenged about the necessity of certain security projects he presented to Regions's executives.

That hasn't happened much in the last few months.

"Before, I used to be seen as a hindrance," Zimmerman says. "What's good now is that the business units are really realizing the importance of security."

Baseline News

Full Story :
http://www.baselinemag.com/article2/0,1540,1986731,00.asp

❖ EU opens public consultation on RFID

Fears about new Radio Frequency Identification technology (RFID), have prompted the EU to open a public consultation process.

The commission has been holding discussions with government agencies and the private sector since March based on general themes of standardising RFID frequencies and formats across Europe, but now the emphasis has changed slightly to inform citizens on how the technology can improve quality of life without encroaching on individual privacy issues. With this in mind, the commission has initiated an online public consultation on its 'Your Voice in Europe' website.

Radio Frequency Identification is a way of storing information on a small tag that communicates via radio frequencies with an electronic reader. It has been applied to hundreds of applications as diverse as tracking migratory birds, embedding information in a passport, to pictures in an art gallery. It does not need line of sight to operate and its distance range depends on the strength of the receiver.

The Register

Full Story :

http://www.theregister.co.uk/2006/07/04/eu_rfid_consultation/

❖ Virus Peril Shifts from E-Mail to Web Sites

BlackSpider warned that the shift towards hosting viruses on the Web will demand a change in security policies. Enterprises commonly filter e-mail messages for viruses and Trojans, and need to expand this with Web filtering techniques to effectively block malware.

New browsers are coming that could make or break your online sales. Read “SSL in High-Security Browsers” to discover the latest best practices for keeping your customers and sales secure.
Malware authors are turning away from e-mail attachments and attempting to lure victims to specially crafted Web sites from which malware is downloaded.

E-mail security vendor BlackSpider Technologies has seen a drop in the number of virus-laden e-mails since the beginning of this year. June set a new record with 0.68 percent of total e-mail traffic, down from 0.73 percent in May.

Total spam volume is also on the decline. Unsolicited messages accounted for 87.7 percent of May's total e-mail traffic and dropped to 78.1 percent in June.

BlackSpider warned that the shift towards hosting viruses on the Web will demand a change in security policies.

SCI-Tech Today

Full Story :
http://www.sci-tech-today.com/story.xhtml?story_id=003000C23UF6

❖ Mobile users face knotty security issues

High-profile security breaches may indicate that network executives are using trial and error to sort out the best ways to secure the brave new world of mobile computing.

In May, headlines blared that personal data on 26 million U.S. military personnel and veterans was at risk after a laptop was stolen from the home of a Department of Veteran Affairs employee.

Last month, the Federal Trade Commission contacted 110 people to tell them that two laptops containing their personal data were stolen from a locked vehicle. The group included defendants in current and past FTC cases.

These and a growing number of similar events show that secure mobile computing is a complex business. The physical devices themselves have to be protected, along with the data stored on them, the users and the network connections, especially wireless.

Network World

Full Story :
http://www.networkworld.com/news/2006/071706-mobile-users-security.html?fsrc=netflash-rss

New Vulnerabilities Tested in SecureScout

❖ 12126 PostgreSQL Set Session Authorization Denial of Service Vulnerability

PostgreSQL Database server is a very popular database server which sees widespread use throughout the world.

PostgreSQL is prone to a remote denial-of-service vulnerability.

An attacker can exploit this issue to cause a loss of service to other database users. Repeated attacks will result in a prolonged denial-of-service condition.

Successful exploitation of this issue requires that the application be compiled with 'Asserts' enabled; this is not the default setting.

PostgreSQL 7.3.x before 7.3.14, 7.4.x before 7.4.12, 8.0.x before 8.0.7, and 8.1.x before 8.1.3 are vulnerable to this issue.

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

References:

# BUGTRAQ:20060215 PostgreSQL security releases 8.1.3, 8.0.7, 7.4.12, 7.3.14
# CONFIRM: http://www.postgresql.org/docs/8.1/static/release.html#RELEASE-8-1-3
# OPENPKG:OpenPKG-SA-2006.004
# URL:http://www.openpkg.org/security/OpenPKG-SA-2006.004-postgresql.html
# TRUSTIX:2006-0008
# URL:http://www.trustix.org/errata/2006/0008
# UBUNTU:USN-258-1
# URL:http://www.ubuntu.com/usn/usn-258-1
# BID:16650
# URL:http://www.securityfocus.com/bid/16650
# FRSIRT:ADV-2006-0605
# URL:http://www.frsirt.com/english/advisories/2006/0605
# SECTRACK:1015636
# URL:http://www.securityfocus.com/archive/1/archive/1/425037/100/0/threaded
# SECUNIA:18890
# URL:http://secunia.com/advisories/18890
# SECUNIA:19015
# URL:http://secunia.com/advisories/19015
# SECUNIA:19035
# URL:http://secunia.com/advisories/19035
# XF:postgresql-setsessionauth-dos(24719)
# URL:http://xforce.iss.net/xforce/xfdb/24719

Home page:
http://www.postgresql.org/

CVE Reference: CVE-2006-0678

❖ 12127 PostgreSQL LOAD Extension Local Privilege Escalation Vulnerability

PostgreSQL Database server is a very popular database server which sees widespread use throughout the world.

A local privilege escalation vulnerability affects PostgreSQL. This issue is due to a failure of the application to restrict critical functionality to privileged users.

An attacker may leverage this issue to execute arbitrary code with the privileges of the affected database, potentially facilitating privilege escalation.

PostgreSQL 7.2.x before 7.2.7, 7.3.x before 7.3.9, 7.4.x before 7.4.7, and 8.0.0 are vulnerable to this issue.

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

References:

# MLIST:[pgsql-bugs] 20050121 Privilege escalation via LOAD
# URL:http://archives.postgresql.org/pgsql-bugs/2005-01/msg00269.php
# MLIST:[pgsql-announce] 20050201 PostgreSQL Security Release
# URL:http://archives.postgresql.org/pgsql-announce/2005-02/msg00000.php

# DEBIAN:DSA-668
# URL:http://www.debian.org/security/2005/dsa-668
# GENTOO:200502-08
# URL:http://security.gentoo.org/glsa/glsa-200502-08.xml
# MANDRAKE:MDKSA-2005:040
# URL:http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:040
# REDHAT:RHSA-2005:138
# URL:http://www.redhat.com/support/errata/RHSA-2005-138.html
# REDHAT:RHSA-2005:150
# URL:http://www.redhat.com/support/errata/RHSA-2005-150.html
# SUSE:SUSE-SA:2005:036
# URL:http://www.novell.com/linux/security/advisories/2005_36_sudo.html
# TRUSTIX:2005-0003
# URL:http://www.trustix.org/errata/2005/0003/
# BUGTRAQ:20050201 [USN-71-1] PostgreSQL vulnerability
# URL:http://marc.theaimsgroup.com/?l=bugtraq&m=110726899107148&w=2
# SECUNIA:12948
# URL:http://secunia.com/advisories/12948

Home page:
http://www.postgresql.org/

CVE Reference: CVE-2006-0678

❖ 12128 PostgreSQL Remote SET ROLE Privilege Escalation Vulnerability

PostgreSQL Database server is a very popular database server which sees widespread use throughout the world.

PostgreSQL is susceptible to a remote privilege-escalation vulnerability. This issue is due to a flaw in the error path of the 'SET ROLE' function.

This issue allows remote attackers with database access to gain administrative access to affected database servers. Since such access also allows filesystem access, other attacks against the underlying operating system may also be possible.

PostgreSQL 8.1.x before 8.1.3 are vulnerable to this issue.

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

References:

# BUGTRAQ:20060215 PostgreSQL security releases 8.1.3, 8.0.7, 7.4.12, 7.3.14
# URL:http://www.securityfocus.com/archive/1/archive/1/425037/100/0/threaded
# MLIST:[pgsql-announce] 20060214 Minor Releases 7.3 thru 8.1 Available to Fix Security Issue
# URL:http://archives.postgresql.org/pgsql-announce/2006-02/msg00008.php
# CONFIRM: http://www.postgresql.org/docs/8.1/static/release.html#RELEASE-8-1-3
# OPENPKG:OpenPKG-SA-2006.004
# URL:http://www.openpkg.org/security/OpenPKG-SA-2006.004-postgresql.html
# CERT-VN:VU#567452
# URL:http://www.kb.cert.org/vuls/id/567452
# BID:16649
# URL:http://www.securityfocus.com/bid/16649

# FRSIRT:ADV-2006-0605
# URL:http://www.frsirt.com/english/advisories/2006/0605
# SECTRACK:1015636
# URL:http://securitytracker.com/id?1015636
# SECUNIA:18890
# URL:http://secunia.com/advisories/18890
# XF:postgresql-setrole-privilege-elevation(24718)
# URL:http://xforce.iss.net/xforce/xfdb/24718

Home page:
http://www.postgresql.org/

CVE Reference: CVE-2006-0553

❖ 12129 PostgreSQL Postmaster Denial Of Service Vulnerability

PostgreSQL Database server is a very popular database server which sees widespread use throughout the world.

PostgreSQL is prone to a denial of service vulnerability. This issue is due to a failure in the application to properly handle exceptional conditions.

A remote attacker can exploit this issue to crash the postmaster service, thus denying future connections until the service is manually restarted.

This issue only affects PostgreSQL for Microsoft Windows.

PostgreSQL 8.0.x before 8.0.6 and 8.1.x before 8.1.2, are vulnerable to this issue.

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

References:

# BUGTRAQ:20060111 PostgreSQL security releases 8.0.6 and 8.1.2
# URL:http://www.securityfocus.com/archive/1/archive/1/421592/100/0/threaded
# MLIST:[pgsql-announce] 20060109 CRITICAL RELEASE: Minor Releases to Fix DoS Vulnerability
# URL:http://archives.postgresql.org/pgsql-announce/2006-01/msg00001.php
# CONFIRM: http://www.postgresql.org/about/news.456
# BID:16201
# URL:http://www.securityfocus.com/bid/16201
# FRSIRT:ADV-2006-0114
# URL:http://www.frsirt.com/english/advisories/2006/0114
# SECTRACK:1015482
# URL:http://securitytracker.com/id?1015482
# SECUNIA:18419
# URL:http://secunia.com/advisories/18419

Home page:
http://www.postgresql.org/

CVE Reference: CVE-2006-0105

❖ 16281 Vulnerability in ASP.NET Could Allow Information Disclosure (MS06-033/917283) (Remote File Checking)

This Information Disclosure vulnerability could allow an attacker to bypass ASP.Net security and gain unauthorized access to objects in the Application folders explicitly by name. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly, but it could be used to produce useful information that could be used to try to further compromise the affected system.

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

References:

Original advisory:
* MS06-033
http://www.microsoft.com/technet/security/bulletin/ms06-033.mspx

Other references:
# BID:18920
# URL:http://www.securityfocus.com/bid/18920
# FRSIRT:ADV-2006-2751
# URL:http://www.frsirt.com/english/advisories/2006/2751
# SECTRACK:1016465
# URL:http://securitytracker.com/id?1016465
# SECUNIA:20999
# URL:http://secunia.com/advisories/20999
# XF:ms-aspnet-appcode-information-disclosure(26802)
# URL:http://xforce.iss.net/xforce/xfdb/26802

CVE Reference: CVE-2006-1300

❖ 16282 Vulnerability in Microsoft Internet Information Services using Active Server Pages Could Allow Remote Code Execution (MS06-034/917537) (Remote File Checking)

There is a remote code execution vulnerability in Internet Information Services (IIS). An attacker could exploit the vulnerability by constructing a specially crafted Active Server Pages (ASP) file, potentially allowing remote code execution if the Internet Information Services (IIS) processes the specially crafted file. 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:
* MS06-034
http://www.microsoft.com/technet/security/bulletin/ms06-034.mspx

Other references:
# CERT-VN:VU#395588
# URL:http://www.kb.cert.org/vuls/id/395588

# BID:18858
# URL:http://www.securityfocus.com/bid/18858
# FRSIRT:ADV-2006-2752
# URL:http://www.frsirt.com/english/advisories/2006/2752
# SECTRACK:1016466
# URL:http://securitytracker.com/id?1016466
# SECUNIA:21006
# URL:http://secunia.com/advisories/21006
# XF:iis-asp-bo(26796)
# URL:http://xforce.iss.net/xforce/xfdb/26796

CVE Reference: CVE-2006-0026

❖ 16283 Vulnerability in Server Service Could Allow Remote Code Execution (MS06-035/917159) (Remote File Checking)

There is a remote code execution vulnerability in the Server driver that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

There is an information disclosure vulnerability in the Server service that could allow an attacker to view fragments of memory used to store SMB traffic during transport.

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

References:

Original advisory:
* MS06-035
http://www.microsoft.com/technet/security/bulletin/ms06-035.mspx

Other references:
* BUGTRAQ:20060711 TSRT-06-02: Microsoft SRV.SYS Mailslot Ring0 Memory Corruption Vulnerability
* URL:http://www.securityfocus.com/archive/1/archive/1/439773/100/0/threaded
* MISC: http://www.tippingpoint.com/security/advisories/TSRT-06-02.html
* CERT-VN:VU#189140
* URL:http://www.kb.cert.org/vuls/id/189140
* XF:win-mailslot-bo(26818)
* URL:http://xforce.iss.net/xforce/xfdb/26818
* BID:18891
* URL:http://www.securityfocus.com/bid/18891
* XF:win-smb-information-disclosure(26820)
* URL:http://xforce.iss.net/xforce/xfdb/26820

CVE Reference: CVE-2006-1314
CVE-2006-1315

❖ 16284 Vulnerability in DHCP Client Service Could Allow Remote Code Execution (MS06-036/914388) (Remote File Checking)

There is a remote code execution vulnerability in the DHCP Client service that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

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

References:

Original advisory:
* MS06-036
http://www.microsoft.com/technet/security/bulletin/ms06-036.mspx

Other references:
# BUGTRAQ:20060711 CYBSEC - Security Pre-Advisory: Microsoft Windows DHCP Client Service Remote Buffer Overflow
# URL:http://www.securityfocus.com/archive/1/archive/1/439675/100/0/threaded
# MISC: http://www.cybsec.com/vuln/CYBSEC-Security_Pre-Advisory_Microsoft_Windows_DHCP_Client_Service_Remote_Buffer_Overflow.pdf
# BID:18923
# URL:http://www.securityfocus.com/bid/18923
# FRSIRT:ADV-2006-2754
# URL:http://www.frsirt.com/english/advisories/2006/2754
# SECUNIA:21010
# URL:http://secunia.com/advisories/21010

CVE Reference: CVE-2006-2372

❖ 16285 Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (MS06-037/917285) (Remote File Checking)

A remote code execution vulnerability exists in Excel that results from the processing of a malformed SELECTION record. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

A remote code execution vulnerability exists in Excel that results from processing of a malformed SELECTION record. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

A remote code execution vulnerability exists in Excel that results from processing of a malformed COLINFO record. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

A remote code execution vulnerability exists in Excel that results from processing of a malformed OBJECT record. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

A remote code execution vulnerability exists in Excel that results from the processing of a malformed FNGROUPCOUNT value file. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

A remote code execution vulnerability exists in Excel that results from the processing of a malformed LABEL record file. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

A remote code execution vulnerability exists in Excel that results from the processing of a malformed file. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

A remote code execution vulnerability exists in Excel that results from the processing of a malformed file. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

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

References:

Original advisory:
* MS06-037
http://www.microsoft.com/technet/security/bulletin/ms06-037.mspx

Other references:
# BUGTRAQ:20060618 Microsoft Excel 0-day Vulnerability FAQ document written
# URL:http://www.securityfocus.com/archive/1/archive/1/437636/100/0/threaded
# BUGTRAQ:20060621 Excel 0-day FAQ updated with Microsoft advisory information
# URL:http://www.securityfocus.com/archive/1/archive/1/437936/100/0/threaded
# MISC: http://blogs.securiteam.com/?p=451
# CONFIRM: http://blogs.technet.com/msrc/archive/2006/06/16/436174.aspx
# CERT:TA06-167A
# URL:http://www.us-cert.gov/cas/techalerts/TA06-167A.html
# MISC: http://isc.sans.org/diary.php?storyid=1420
# CERT-VN:VU#802324
# URL:http://www.kb.cert.org/vuls/id/802324
# BID:18422
# URL:http://www.securityfocus.com/bid/18422
# FRSIRT:ADV-2006-2361
# URL:http://www.frsirt.com/english/advisories/2006/2361
# OSVDB:26527
# URL:http://www.osvdb.org/26527
# SECTRACK:1016316
# URL:http://securitytracker.com/id?1016316
# SECUNIA:20686
# URL:http://secunia.com/advisories/20686
# XF:excel-unspecified-code-execution(27179)
# URL:http://xforce.iss.net/xforce/xfdb/27179

CVE Reference: CVE-2006-1301
CVE-2006-1302
CVE-2006-1304
CVE-2006-1306
CVE-2006-1308
CVE-2006-1309
CVE-2006-2388
CVE-2006-3059

❖ 16286 Vulnerabilities in Microsoft Office Could Allow Remote Code

Execution (MS06-038/917284) (Remote File Checking)

A remote code execution vulnerability exists in Office, and could be exploited when a malformed string included in an Office file was parsed by any of the affected Office applications. Such a string might be included in an email attachment processed by one of the affected applications or hosted on a malicious web site. Viewing or previewing a malformed email message in an affected version of Outlook could not lead to exploitation of this vulnerability. An attacker could exploit the vulnerability by constructing a specially crafted Office file that could allow remote code execution.

A remote code execution vulnerability exists in Office, and could be exploited when a malformed string included in an Office file was parsed by any of the affected Office applications. Such a string might be included in an email attachment processed by one of the affected applications or hosted on a malicious web site. Viewing or previewing a malformed email message in an affected version of Outlook could not lead to exploitation of this vulnerability. An attacker could exploit the vulnerability by constructing a specially crafted Office file that could allow remote code execution.

A remote code execution vulnerability exists in Office, and could be exploited when a malformed property included in an Office file was parsed by any of the affected Office applications. Such a property might be included in an email attachment processed by one of the affected applications or hosted on a malicious web site. Viewing or previewing a malformed email message in an affected version of Outlook could not lead to exploitation of this vulnerability. An attacker could exploit the vulnerability by constructing a specially crafted Office file that could allow remote code execution.

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

References:

Original advisory:
* MS06-038
http://www.microsoft.com/technet/security/bulletin/ms06-038.mspx

Other references:
* CERT-VN:VU#580036
* URL:http://www.kb.cert.org/vuls/id/580036
* FRSIRT:ADV-2006-2756
* URL:http://www.frsirt.com/english/advisories/2006/2756
* SECUNIA:21012
* URL:http://secunia.com/advisories/21012
* XF:office-string-parse-bo(27607)
* URL:http://xforce.iss.net/xforce/xfdb/27607
* MISC: http://www.milw0rm.com/exploits/1615
* BID:17252
* URL:http://www.securityfocus.com/bid/17252
* SECTRACK:1015855
* URL:http://securitytracker.com/id?1015855
* XF:office-property-string-bo(27609)
* URL:http://xforce.iss.net/xforce/xfdb/27609
* CERT-VN:VU#409316
* URL:http://www.kb.cert.org/vuls/id/409316

CVE Reference: CVE-2006-1316

CVE-2006-1540
CVE-2006-2389

❖ 16287 Vulnerabilities in Microsoft Office Filters Could Allow Remote Code Execution (MS06-039/915384) (Remote File Checking)

A remote code execution vulnerability exists in Office and could be exploited when Office opened a malformed PNG file. An attacker could exploit the vulnerability by constructing a specially crafted PNG file that could allow remote code execution.

A remote code execution vulnerability exists in Office and could be exploited when a user opened a malformed GIF file. An attacker could exploit the vulnerability by constructing a specially crafted GIF file that could allow remote code execution.

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

References:

Original advisory:
* MS06-039
http://www.microsoft.com/technet/security/bulletin/ms06-039.mspx

Other references:
* CERT-VN:VU#668564
* URL:http://www.kb.cert.org/vuls/id/668564
* BID:18915
* URL:http://www.securityfocus.com/bid/18915
* FRSIRT:ADV-2006-2757
* URL:http://www.frsirt.com/english/advisories/2006/2757
* SECUNIA:21013
* URL:http://secunia.com/advisories/21013
* CERT-VN:VU#459388
* URL:http://www.kb.cert.org/vuls/id/459388
* BID:18913
* URL:http://www.securityfocus.com/bid/18913

CVE Reference: CVE-2006-0033
CVE-2006-0007

New Vulnerabilities found this Week

Multiple Microsoft Vulnerabilities.

Vulnerability in ASP.NET Could Allow Information Disclosure (MS06-033/917283)
Vulnerability in Microsoft Internet Information Services using Active Server Pages Could Allow Remote Code Execution (MS06-034/917537)
Vulnerability in Server Service Could Allow Remote Code Execution (MS06-035/917159)
Vulnerability in DHCP Client Service Could Allow Remote Code Execution (MS06-036/914388)
Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (MS06-037/917285)
Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS06-038/917284)

Vulnerabilities in Microsoft Office Filters Could Allow Remote Code Execution (MS06-039/915384) (Remote File Checking)

References:
http://www.microsoft.com/technet/security/bulletin/ms06-033.mspx
http://www.microsoft.com/technet/security/bulletin/ms06-034.mspx
http://www.microsoft.com/technet/security/bulletin/ms06-035.mspx
http://www.microsoft.com/technet/security/bulletin/ms06-036.mspx
http://www.microsoft.com/technet/security/bulletin/ms06-037.mspx
http://www.microsoft.com/technet/security/bulletin/ms06-038.mspx
http://www.microsoft.com/technet/security/bulletin/ms06-039.mspx
http://descriptions.securescout.com/tc/16281
http://descriptions.securescout.com/tc/16282
http://descriptions.securescout.com/tc/16283
http://descriptions.securescout.com/tc/16284
http://descriptions.securescout.com/tc/16285
http://descriptions.securescout.com/tc/16286
http://descriptions.securescout.com/tc/16287

Cisco IPS Packet Handling Denial of Service Vulnerability

"Denial of Service"

A vulnerability has been reported in Cisco Intrusion Prevention System (IPS), which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the custom device driver for Intel-based gigabit network adapters when processing certain malformed IP packets. This can be exploited to cause a DoS via a specially crafted packet received on an Intel-based gigabit network adapter configured as a sensing interface.

Successful exploitation causes the network device to stop processing packets and become inaccessible both remotely and via the console.

The vulnerability affects 42xx appliances running IPS software version 5.1 (see the vendor advisory for a full list of vulnerable devices).
References:
http://www.cisco.com/warp/public/707/cisco-sa-20060712-ips.shtml

Cisco Router Web Setup Insecure Default Cisco IOS Configuration

"Execute arbitrary commands with privilege level 15"

A security issue has been reported in Cisco Router Web Setup, which potentially can be exploited by malicious people to compromise a vulnerable system.

The problem is caused due to the application shipping with an insecure default Cisco IOS configuration. This can be exploited to execute arbitrary commands with privilege level 15 via the web interface.

The security issue has been reported in versions prior to 3.3.0 build 31.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20060712-crws.shtml

Adobe Acrobat / Adobe Reader Insecure Default Permissions

"Gain escalated privileges"

A vulnerability has been reported in Adobe Acrobat and Adobe Reader, which can be exploited by malicious, local users to bypass certain security restrictions or gain escalated privileges.

The vulnerability is caused due to insecure default file permissions being set on the installed files and folders. This allows any non-privileged users on the system to remove the files or replace them with malicious binaries.

The vulnerability has been reported for Adobe Acrobat 6.0.4 and Adobe Reader 6.0.4 for Mac OS. Prior versions may be also affected.

References:
http://www.adobe.com/support/security/bulletins/apsb06-08.html

Adobe Acrobat Buffer Overflow Vulnerability

"Execution of arbitrary code"

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

The vulnerability is caused due to a boundary error when distilling files to PDF. This can be exploited to cause a buffer overflow via a specially crafted file.

Successful exploitation allows execution of arbitrary code.

The vulnerability has been reported in versions 6.0 through 6.0.4 for Windows and Macintosh.

References:
http://www.adobe.com/support/security/bulletins/apsb06-09.html

Juniper Networks JUNOS IPv6 Packet Handling Denial of Service

"Denial of Service"

A vulnerability has been reported in the M-series, T-series, and J-Series routers, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error when freeing memory after receiving certain IPv6 packets. This can be exploited to cause a exhaust available memory by sending specially crafted IPv6 packets to the vulnerable router.

Successful exploitation crashes the router.

The vulnerability has been reported for routers using a version of the JUNOS Internet Software built before 2006-05-10.

References:
http://www.juniper.net/support/security/alerts/IPv6_bug.txt

http://www.juniper.net/support/security/alerts/EXT-PSN-2006-06-017.txt

Samba Multiple Share Connection Requests Denial of Service

"Denial of Service"

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

The vulnerability is caused due to an error when handling a lot of share connection requests. This can be exploited to cause smbd to exhaust memory resources via a large number of share connections.

The vulnerability has been reported in versions 3.0.1 through 3.0.22.

References:
http://us1.samba.org/samba/security/CAN-2006-3403.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