netVigilance

ScoutNews Team

August 12, 2005
Issue # 32

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review
Top Security News Stories this Week
New Test Cases Tested in SecureScout
New Vulnerabilities this Week

This Week in Review

Consumer Reports survey on home PC security is out, Spyware trend takes a sinister turn, business mute on extent of cyber-attacks and universities become huge target for identity thieves.

Enjoy reading

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

❖ Home PCs extremely vulnerable to costly attacks

The Consumer Reports *State of the net Survey.* The report gives statistics on the nature of the threats facing home pc users. Not all is bad news, the report also includes a great list of best practices for strengthening your home pc security.

Consumer Reports

Full Story :

http://www.consumeraffairs.com/news04/2005/cr_web.html

❖ Disturbing trend in spyware uncovered

A Trojan horse application to steal sensitive financial and personal information and send it to a remote server. "It's totally geared for stealing users' accounts and identity information--everything [the criminals] need to get new credit cards in your name and empty out your bank accounts," according to Eric Sites, Sunbelt's vice president of research and development

Another Trojan Horse exploit, quietly sleep on infected systems and when launched, displays a swastika and a Nazi slogan.

This could indicate a chilling trend in the nature of hard to detect malware Trojans. Fixes are still pending for both Trojans.

Full Story :
http://news.yahoo.com/news?tmpl=story&u=/pcworld/20050810/tc_pcworld/122176

❖ FBI – Corporate cyber attacks go largely unreported

FBI Director, Robert Mueller reported at the annual meeting of the InfraGard national conference in Washington D.C., that most cyber crime incidents against businesses go unreported.

The reasons are varied mostly driven by fear. Companies feel that their business will suffer from customer defection or by a competitors exploitation of the information.
Associated Press

Related Links:
http://news.yahoo.com/news?tmpl=story&u=/ap/20050809/ap_on_hi_te/computer_security
http://p2pnet.net/story/5872

❖ Spate of identity thefts hit universities

Sonoma State University in California, the University of North Texas and the University of Colorado at Boulder all reported cases of electronic break-in that resulted in loss of personal identity data.

Universities are prime targets since their data security is not a high priority, access is required by tens of thousands of users and the alumni typically represent the fruitful gainfully employed middle and upper class.
Source

Related Links:
http://www.internetweek.com/news/168600607
http://news.yahoo.com/s/afp/20050809/tc_afp/usinternetfraud_050809233713
http://www.kxtv10.com/storyfull1.asp?id=12469
http://www.colorado.edu/its/security/whc/
http://www.signonsandiego.com/uniontrib/20040507/news_7m7breach.html

New Vulnerabilities Tested in SecureScout

- ❖ **15675 Cisco IOS IPv6 Crafted Packet Vulnerability (CSCef68324)**

A vulnerability exists in the processing of IPv6 packets. Crafted packets from the local segment received on logical interfaces (that is, tunnels including 6to4 tunnels) as well as physical interfaces can trigger this vulnerability. Crafted packets can not traverse a 6to4 tunnel and attack a box across the tunnel.

The crafted packet must be sent from a local network segment to trigger the attack. This vulnerability can not be exploited one or more hops from the IOS device.

Successful exploitation of the vulnerability on Cisco IOS may result in a reload of the device or execution of arbitrary code. Repeated exploitation could result in a sustained DoS attack or execution of arbitrary code on Cisco IOS devices.

Successful exploitation of the vulnerability on Cisco IOS-XR may result in a restart of the IPv6 neighbor discovery process. A restart of this process will only affect IPv6 traffic passing through the system. All other processes and traffic will be unaffected. Repeated exploitation could result in a sustained DoS attack on IPv6 traffic.

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

References:

Original Advisory:
Cisco IOS IPv6 Crafted Packet Vulnerability (CSCef68324):
http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml

Other References:
US-CERT VU#930892:
http://www.kb.cert.org/vuls/id/930892

CVE Reference: CAN-2005-2451

- ❖ **15676 Cisco IOS RADIUS Authentication Bypass (CSCee45312)**

Remote Authentication Dial In User Service (RADIUS) authentication on a device that is running certain versions of Cisco Internetworking Operating System (IOS) and configured with a fallback method to none can be bypassed.

Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected.

Only the systems that are running certain versions of Cisco IOS are affected. Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.

Successful exploitation of the vulnerability may result in bypassing the RADIUS authentication.

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

References:

Original Advisory:
Cisco IOS RADIUS Authentication Bypass (CSCee45312):
http://www.cisco.com/warp/public/707/cisco-sa-20050629-aaa.shtml

CVE Reference: CAN-2005-2105

❖ 15677 Cumulative Security Update for Internet Explorer (MS05-038/896727)

A remote code execution vulnerability exists in Internet Explorer because of the way that it handles JPEG images. An attacker could exploit the vulnerability by constructing a malicious JPEG image that could potentially allow remote code execution if a user visited a malicious Web site or viewed a malicious e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A cross-domain vulnerability exists in Internet Explorer that could allow information disclosure or remote code execution on an affected system. An attacker could exploit the vulnerability by constructing a malicious Web page. The malicious Web page could potentially allow remote code execution if it is viewed by a user. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, significant user interaction and social engineering is required to exploit this vulnerability.

A remote code execution vulnerability exists in the way Internet Explorer instantiates COM Objects that are not intended to be used in Internet Explorer. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited the malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References:

http://www.microsoft.com/technet/security/Bulletin/MS05-038.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1988
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1989
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1990

CVE Reference: CAN-2005-1988, CAN-2005-1989, CAN-2005-1990

❖ 15678 Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (MS05-039/899588)

A remote code execution and local elevation of privilege vulnerability exists in Plug and Play 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: **High** Risk: **Attack**

References:

http://www.microsoft.com/technet/security/Bulletin/MS05-039.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1983

CVE Reference: CAN-2005-1983

❖ 15679 Vulnerability in Telephony Service Could Allow Remote Code Execution (MS05-040/893756)

A remote code execution vulnerability exists in Telephony Application Programming Interface (TAPI) 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: **High** Risk: **Attack**

References:

http://www.microsoft.com/technet/security/Bulletin/MS05-040.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0058

CVE Reference: CAN-2005-0058

❖ 15680 Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (MS05-041/899591)

A denial of service vulnerability exists that could allow an attacker to send a specially crafted Remote Data Protocol (RDP) message to an affected system. An attacker could cause this system to stop responding.

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

References:

http://www.microsoft.com/technet/security/Bulletin/MS05-041.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1218

CVE Reference: CAN-2005-1218

❖ 15681 Vulnerabilities in Kerberos Could Allow Denial of Service, Information Disclosure, and Spoofing (MS05-042/899587)

A denial of service vulnerability exists that could allow an attacker to send a specially crafted message to a Windows domain controller that could cause the service that is responsible for authenticating users in an Active Directory domain to stop responding.

This is an information disclosure and spoofing vulnerability. This vulnerability could allow an attacker to tamper with certain information that is sent from a domain controller and potentially access sensitive client network communication. Users could believe they are accessing a trusted server when in reality they are accessing a malicious server. However, an attacker would first have to inject themselves into the middle of an authentication session between a client and a domain controller.

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

References:

http://www.microsoft.com/technet/security/Bulletin/MS05-042.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1981
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1982

CVE Reference: CAN-2005-1981, CAN-2005-1982

❖ 15682 Vulnerability in Print Spooler Service Could Allow Remote Code Execution (MS05-043/896423)

A remote code execution vulnerability exists in the Printer Spooler 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: **High** Risk: **Attack**

References:

http://www.microsoft.com/technet/security/Bulletin/MS05-043.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1984

CVE Reference: CAN-2005-1984

❖ 16103 ProFTPD Server Response Filtering Weakness

ProFTPD is an FTP server available for many Unix platforms.

It has been reported that multiple vendor's servers are affected by a server response splitting weakness.

An attacker may leverage these issues to have attacker-specified data echoed back to the computer that the request originated from. This may facilitate various attacks including cross-site scripting attacks in Web browsers through concurrent exploitation of the issues outlined in BID 3181 (Multiple Vendor HTML Form Protocol Vulnerability).

The vulnerability affects versions up to 1.2.9.

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

References:

Original Advisory:
http://eyeonsecurity.org/papers/extendedform.pdf

Other references:
http://securityfocus.com/bid/11655

Product page:
http://www.proftpd.org/

CVE Reference: None

- ❖ 16104 **ProFTPD Authentication Delay Username Enumeration Vulnerability**

ProFTPD is an FTP server available for many Unix platforms.

A timing attack is described in ProFTPD that could assist a remote user in enumerating usernames.

A remote attacker may exploit this vulnerability to determine what usernames are valid, privileged, or do not exist on the remote system.

The vulnerability affects versions up to 1.2.9 rc3

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

References:

Original Advisory:
http://security.lss.hr/en/index.php?page=details&ID=LSS-2004-10-02

Other references:
http://securityfocus.com/archive/1/378518
http://securityfocus.com/bid/11430

Product page:
http://www.proftpd.org/

CVE Reference: None

New Vulnerabilities found this Week

- ❖ **Linksys WLAN Monitor Privilege Escalation Vulnerability**
  "Gain escalated privileges"

Reed Arvin has discovered a vulnerability in Linksys WLAN Monitor, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to the program running its GUI with SYSTEM privileges rather than using the privilege of the currently logged on user. This can be exploited gain SYSTEM privileges by invoking the program from the system tray and then using its profile import file open dialog box to launch cmd.exe.

The vulnerability has been confirmed in version 2.0. Other versions may also be affected.

References:
http://reedarvin.thearvins.com/20050810-01.html

- **GNOME Evolution Multiple Format String Vulnerabilities**
  “Execute arbitrary code”

Ulf Harnhammar has reported some vulnerabilities in Evolution, which can be exploited by malicious people to compromise a vulnerable system.

1) A format string error when displaying full vCard information attached to an e-mail message can be exploited to execute arbitrary code.

Successful exploitation requires that the user clicks on "Show Full vCard" or saves the vCard to an address book and then views it under the "Contacts" tab.

2) A format string error exists when displaying specially crafted contact data retrieved from an LDAP server.

3) A format string error exists when displaying specially crafted task list data retrieved from remote servers and when the user saves the task list data under the "Calendars" tab.

The vulnerabilities have been reported in versions 1.5 through 2.3.6.1.

References:
http://www.sitic.se/eng/advisories_and_recommendations/sa05-001.html

- **Nortel VPN Client Privilege Escalation Vulnerability**
  “Gain escalated privileges”

Jeff Peadro has discovered a vulnerability in Nortel VPN Client, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to the program running its GUI with SYSTEM privileges rather than using the privileges of the currently logged on user. This can be exploited to gain SYSTEM privileges by using the certificate or token selection functionality to launch cmd.exe.

Successful exploitation requires that the client has been installed as a system service.

The vulnerability has been confirmed in version 04_65.26 and also reported in version 05_01.030. Other versions may also be affected.

References:
http://secunia.com/advisories/16376/

- **Gaim Away Message Buffer Overflow and Denial of Service**
  "Denial of Service; Execution of arbitrary code"

A vulnerability and a weakness have been reported in Gaim, which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a user's system.

1) An error in the handling of away messages can be exploited to cause a heap-based buffer overflow by sending a specially crafted away message to a user logged into AIM or ICQ.

Successful exploitation allows execution of arbitrary code.

2) An error in the handling of file transfers can be exploited to crash the application by attempting to upload a file with a non-UTF8 filename to a user logged into AIM or ICQ.

References:
http://sourceforge.net/tracker/index.php?func=detail&aid=1235427&group_id=235&atid=100235
http://rhn.redhat.com/errata/RHSA-2005-627.html

- **Internet Explorer Three Vulnerabilities**
  "Conduct cross-site scripting attacks; Execute arbitrary code"

Three vulnerabilities have been reported in Internet Explorer, which can be exploited by malicious people to conduct cross-site scripting attacks or compromise a user's system.

1) A memory corruption error within the processing of JPEG images can be exploited to execute arbitrary code by tricking a user into e.g. visiting a web site or view an HTML e-mail containing a specially crafted JPEG image.

2) A validation error during the interpretation of certain URLs when

browsing from a web site to a web folder view using WebDAV can be exploited to execute arbitrary script code in another domain (e.g. on the user's system in the "Local Machine" security zone).

3) An error in the way COM objects are instantiated as ActiveX controls can be exploited to corrupt system memory and allows execution of arbitrary code on a user's system when e.g. a malicious web site is visited.

References:
http://www.microsoft.com/technet/security/Bulletin/MS05-038.mspx
http://support.microsoft.com/kb/896727
http://www.kb.cert.org/vuls/id/965206
http://www.kb.cert.org/vuls/id/959049

- **Microsoft Windows Plug-and-Play Service Buffer Overflow**
  "Gain escalated privileges"

ISS X-Force has reported a vulnerability in Microsoft Windows, which can be exploited by malicious users to gain escalated privileges or by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the Plug-and-Play service and can be exploited to cause a stack-based buffer overflow.

Successful exploitation allows malicious users to gain escalated privileges. On Windows 2000, the vulnerability can be exploited by malicious people to execute arbitrary code without requiring valid user credentials.

References:
http://www.microsoft.com/technet/security/Bulletin/MS05-039.mspx
http://xforce.iss.net/xforce/alerts/id/202
http://www.kb.cert.org/vuls/id/998653

- **Microsoft Windows Two Kerberos Vulnerabilities**
  "Denial of Service"

Two vulnerabilities have been reported in Microsoft Windows, which can be exploited by malicious users to cause a DoS (Denial of Service), reveal sensitive information, or impersonate other users.

1) An unspecified error in the handling of special Kerberos messages allows malicious users to cause the domain controller to shutdown.

This vulnerability only affects Microsoft Windows Server 2000 and 2003, which are configured as domain controllers.

2) An unspecified error in the handling of PKINIT transactions, may allow users to impersonate other users by conducting a MITM (Man In The Middle) attack.

This only affects systems using SmartCard authentication.

References:
http://www.microsoft.com/technet/security/Bulletin/MS05-042.mspx
http://www.kb.cert.org/vuls/id/610133

- ❖ **Sun Solaris printd Daemon Arbitrary File Deletion Vulnerability**
  "Delete files on a vulnerable system"

A vulnerability has been reported in Solaris, which can be exploited by malicious users to delete files on a vulnerable system.

The vulnerability is caused due to an unspecified error in the printd daemon and makes it possible to delete an arbitrary file with the privileges of the user running the printd daemon.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101842-1

- ❖ **Microsoft Windows Telephony Service Vulnerability**
  "Gain escalated privileges"

A vulnerability has been reported in Microsoft Windows, which can be exploited by malicious, local users to gain escalated privileges or by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an unspecified error in the TAPI (Telephony Application Programming Interface) service when validating permissions and the length of certain messages before copying the data to an allocated buffer.

Successful exploitation allows malicious, local users to gain escalated privileges. On certain configurations of Windows 2000 Server and Windows Server 2003 with the Telephony service enabled (disabled by default), it is also possible to exploit the vulnerability without a local account. However, only authenticated users can access the service on Windows Server 2003 and hence exploit the vulnerability.

References:
http://www.microsoft.com/technet/security/Bulletin/MS05-040.mspx

- ❖ **Linux Kernel Keyring Management 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 within the handling of keyrings makes it possible to crash the kernel when destroying a keyring that wasn't properly instantiated. This can be exploited by attempting to add a keyring that doesn't have an empty payload.

2) An error within the error handling path for the "KEYCTL_JOIN_SESSION_KEYRING" operation when attempting to join a key management session may cause the session management semaphore to not be released. This can be exploited by attempting to add a new session keyring.

References:
http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.13-rc6

❖ **Linux Kernel xfrm Array Indexing Overflow Vulnerability**
"Denial of Service"

Balazs Scheidler has reported a vulnerability in the Linux kernel, which potentially can be exploited by malicious, local users to cause a DoS (Denial of Service).

The vulnerability is caused due to a boundary error in the XFRM code and can be exploited to cause an array indexing overflow.

References:
http://www.mail-archive.com/netdev@vger.kernel.org/msg00520.html
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12.4

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