netVigilance

ScoutNews Team

November 18, 2005
Issue # 46

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

I love it when this stuff writes itself – the SONY XCP rootkit remover is a far more dangerous rootkit than the original !? loss of data equals loss of customers, Iowa State University wants to be hacked and FBI/CSI '05 data hits the press.

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

- **SONY continues rootkit blunders**

Responding to industry and consumer backlash, SONY announced earlier this week that it will recall products containing the XCP application and released a de-installation script available from its website.

This is where the whole situation goes from bad to worse for the not-so-nimble giant. Ed Felten, a Princeton University professor of computer science warns that the rootkit remover published by SONY-BMG allows any website to run code onto a PC and take command of it. (Full Story)

SONY is calling the temporary suspension of the manufacture of CD's containing XCP as (you're gonna' love this), a 'precautionary measure'. I guess it's not called the ‘entertainment’ business for nothing, but the keystone kops went out with talkies guys?

In an interview (audio, commentary) with NPR; Sony BMG's president of global digital business; Thomas Hesse demonstrated the company's disdain for its customers when he said, 'Most people don't even know what a rootkit is, so why should they care about it?' Weblogs are sprouting up calling for a boycott of SONY.

I guess that IP protection will be ensured when no one wants to buy your products. – *Ed.*

Related Links:
http://www.scmagazine.com/us/news/article/527622/?s=nus
http://www.scmagazine.com/us/news/article/528039/?s=nus
http://antivirus.about.com/od/virusdescriptions/a/sonypres.htm

❖ Consumers revolt against firms that lose data

The results of two separate surveys concerning data loss by corporations find that losses for these companies can be very severe, with 19 percent stating that they immediately cancelled accounts with sloppy firms and another 40 percent considering it.

Encryption vendor PGP Corp. conducted the surveys, one polling consumers and another targeting companies. PGP estimated the cost per breach to be $14 million and roughly 23 million Americans have been notified of mishandling of their personal information in the last 12 months.
TechWeb News

Full Story :
http://www.techweb.com/wire/ebiz/173602532%3bjsessionid=3BO2APLQ3QPUAQSNDBNSKH0CJUMEKJVN

❖ Iowa State University welcomes hacking

In an effort to give computer science students practical, real world experience in fending off hacker attacks. ISU’s second annual second cyber defense competition will pit 3 teams of defenders against a team representing hackers launching attacks against their networks.
Source

Full Story:

http://iasg.ece.iastate.edu/cdc/
http://www.ksl.com/?nid=148&sid=129346

❖ Data on trends in Cyber crime

Interesting data on emerging trends is computer crime from the new face of hackers, FBI/CSI 2005 survey results and a report on the [in]effectiveness of the criminal justice system in prosecuting these types of crimes. Worth the read.

Related Links:
http://singe.rucus.net/blog/archives/574-Computer-Crime-Trends.html

New Vulnerabilities Tested in SecureScout

❖ 13313 Oracle Database Server - Oracle Spatial component Unspecified error (oct-2005/DB22)

An unspecified error in the Oracle Spatial component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

Product Homepage:
http://www.oracle.com/

CVE Reference: CAN-2005-0873

❖ 13314 Oracle Database Server - Oracle Spatial component Unspecified error (oct-2005/DB23)

An unspecified error in the Oracle Spatial component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

Product Homepage:
http://www.oracle.com/

CVE Reference: CAN-2005-0873

❖ 13315 Oracle Database Server - Oracle Spatial component Unspecified error (oct-2005/DB24)

An unspecified error in the Oracle Spatial component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

Product Homepage:
http://www.oracle.com/

CVE Reference: CAN-2005-0873

❖ 13316 Oracle Database Server - Oracle Spatial component Unspecified error (oct-2005/DB25)

An unspecified error in the Oracle Spatial component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

Product Homepage:
http://www.oracle.com/

CVE Reference: CAN-2005-0873

❖ 13317 Oracle Database Server - Programmatic Interface component Unspecified error (oct-2005/DB26)

An unspecified error in the Programmatic Interface component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

Product Homepage:
http://www.oracle.com/

CVE Reference: CAN-2005-0873

❖ 16032 HP Web Based Management Software HTTP Server Buffer Overflow

Some Compaq/HP systems are delivered with a pre-installed web server, which is part of Compaq Management Agents and the Compaq Survey Utility and listens to port 2301.

A vulnerability has been reported in HP HTTP Server, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an unspecified boundary error within the handling of input parameters and can be exploited to cause a buffer overflow.

Successful exploitation may allow execution of arbitrary code.

The vulnerability affects HP web-enabled management products running HP HTTP Server versions 4.0 through 5.95.

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

References:

Original advisory:

http://itrc.hp.com/service/cki/docDisplay.do?docId=HPSBMA01116

Other references:

http://secunia.com/advisories/14311/

Management Software Security Patch for Windows Version 5.96:

http://h18023.www1.hp.com/support/files/Server/us/download/22192.html

CVE Reference: None

❖ 16033 HP Web Based Management Anonymous Certificate Upload Vulnerability

Some Compaq/HP systems are delivered with a pre-installed web server, which is part of Compaq Management Agents and the Compaq Survey Utility and listens to port 2301.

Dave Aitel has discovered a vulnerability in HP HTTP server, allowing malicious people to gain access to administrative functions.

The problem is that if HP HTTP has been configured to accept "Anonymous Access", it is possible to upload a client certificate, which will be accepted as a valid certificate for authorisation. This can be exploited by malicious people to gain access to administrative functions.

The vulnerability affects all HP Web Based Management Products running HP HTTP versions 5.0 through 5.92.

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

References:

Original advisory:
http://www.immunitysec.com/downloads/hp_http.sxw.pdf
http://h18023.www1.hp.com/support/files/Server/us/download/20197.html

Other references:
http://secunia.com/advisories/11126/

Version 5.93 available at:
http://h18023.www1.hp.com/support/files/Server/us/download/20197.html

CVE Reference: None

❖ 16034 HP Web Based Management multiple OpenSSL Vulnerabilities

Some Compaq/HP systems are delivered with a pre-installed web server, which is part of Compaq Management Agents and the Compaq Survey Utility and listens to port 2301.

Incorporated OpenSSL has multiples vulnerabilities.

The vulnerability affects all HP Web Based Management Products running HP HTTP versions 5.0 through 5.93

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

References:

Original advisory:
http://h18007.www1.hp.com/support/files/server/us/download/20666.html

Other references:

Version 5.94 available at:
http://h18007.www1.hp.com/support/files/server/us/download/20666.html

CVE Reference: None

❖ 16035 Cisco IOS IOS Heap-based Overflow Vulnerability in System Timers (CSCei61732)

Cisco IOS may be susceptible to remote code execution through attack vectors such as specific heap-based overflows in which internal operating system timers may execute arbitrary code from portions of memory that have been overwritten via exploitation.

In many cases, a heap-based overflow in Cisco IOS will simply corrupt system memory and trigger a system reload when detected by the "Check Heaps" process, which constantly monitors for such memory corruption. In a successful attack against an appropriate heap-based overflow, it is possible to achieve code execution without the device crashing immediately.

Successful exploitations of heap-based buffer overflow vulnerabilities in Cisco IOS software often result in a Denial of Service because the exploit causes the router to crash and reload due to inconsistencies in running memory. In some cases it is possible to overwrite areas of system memory and execute arbitrary code from those locations. In the event of successful remote code execution, device integrity will have been completely compromised.

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

References:

Original Advisory:
Cisco IOS IOS Heap-based Overflow Vulnerability in System Timers (CSCei61732):
http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml

Other References:
US-CERT VU#562945:
http://www.kb.cert.org/vuls/id/562945

http://secunia.com/advisories/17413/

CVE Reference: None

❖ 16036 Cisco IOS Firewall Authentication Proxy for FTP and Telnet (CSCsa54608)

The Cisco IOS Firewall Authentication Proxy feature allows network administrators to apply specific security policies on a per-user basis. With the Firewall Authentication Proxy for FTP and/or Telnet Sessions feature, users can log into the network services via FTP and/or Telnet, and their specific access profiles are automatically retrieved and applied from a Remote Authentication Dial In User Service (RADIUS), or Terminal Access Controller Access Control System Plus (TACACS+) authentication server.

Cisco IOS Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack when processing the user authentication credentials from an Authentication Proxy Telnet/FTP session. To exploit this vulnerability an attacker must first complete a TCP connection to the IOS device running affected software and receive an auth-proxy authentication prompt.

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.

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

References:

Original Advisory:
Cisco IOS Firewall Authentication Proxy for FTP and Telnet (CSCsa54608):
http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml

Other References:
US-CERT VU#236045:
http://www.kb.cert.org/vuls/id/236045

http://secunia.com/advisories/16719/

CVE Reference: None

New Vulnerabilities found this Week

Cisco Wireless IP Phone Two Vulnerabilities
"Denial of Service**"**

Two vulnerabilities have been reported in Cisco Wireless IP Phone, which can be exploited by malicious people to gain access to potentially sensitive information, to modify certain information, and to cause a DoS (Denial of Service).

1) The SNMP service that runs on the IP phone uses fixed read-only and read-write community strings of "public" and "private", which cannot be changed by the user. This can be exploited to retrieve and modify the device configuration, including stored user data such as phone book entries by sending SNMP GetRequest or SetRequest to phone.

2) The IP phone listens on port 17185/udp to allow connections from the VxWorks debugger. This may be exploit to collect debugging information or to cause a DoS on the device.

The vulnerabilities have been reported in Cisco 7920 Wireless IP Phone with firmware version 2.0 and prior.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20051116-7920.shtml

Microsoft Windows UPnP GetDeviceList Denial of Service
"Denial of Service"

Winny Thomas has discovered a vulnerability in Microsoft Windows, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to a memory allocation error when handling UPnP GetDeviceList requests via RPC. This can be exploited to cause "services.exe" to consume large amount of memory for a limited period of time.

Successful exploitation causes a DoS but requires valid logon credentials on Windows XP Service Pack 1.

The vulnerability has been confirmed in Windows 2000 SP4 and is also reported in Windows XP Service Pack 1.

Note: An exploit for this vulnerability is publicly available.

References:
http://www.microsoft.com/technet/security/advisory/911052.mspx

Macromedia Flash Communication Server MX Denial of Service
“Denial of Service”

A vulnerability has been reported in Macromedia Flash Communication Server MX, which potentially can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability has been reported in the following versions:
* Flash Communication Server MX 1.0 (all editions)
* Flash Communication Server MX 1.5 (all editions)

References:
http://www.macromedia.com/devnet/security/security_zone/mpsb05-09.html
http://secunia.com/advisories/17611/

Sony CD First4Internet XCP Uninstallation ActiveX Control Vulnerability
“Install arbitrary code”

A vulnerability has been reported in First4Internet XCP's uninstallation ActiveX control, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to the "CodeSupport.ocx" ActiveX control that is installed via Internet Explorer when the user un-installs the XCP DRM software by visiting the vendor's website. The ActiveX control is marked safe-for-scripting and supports several potentially dangerous methods like "RebootMachine", "InstallUpdate", and "IsAdministrator". This may be exploited to install arbitrary code on the user's system.

Successful exploitation requires that the user visits a malicious website.

References:
http://www.freedom-to-tinker.com/?p=927
http://hack.fi/~muzzy/sony-drm/
http://www.kb.cert.org/vuls/id/312073

Nortel Switched Firewall ISAKMP IKE Message Processing Denial of Service

"Denial of Service"

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

The vulnerability is caused due to unspecified errors in the processing of IKEv1 Phase 1 protocol exchange messages. This may be exploited to cause a DoS via specially crafted IKE packets.

References:
http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=BLTNDETAIL&DocumentOID=367651&RenditionID=

Internet Explorer Image Control Status Bar Spoofing Weakness

"Visiting a malicious website by obfuscating URLs displayed in the status bar"

Claudio "Sverx" has discovered a weakness in Internet Explorer, which can be exploited by malicious people to trick users into visiting a malicious website by obfuscating URLs displayed in the status bar.

The problem is that the browser fails to show the correct URL in the status bar if an image control has been enclosed in a hyperlink and uses a form to specify the destination URL. This may cause a user to follow a link to a seemingly trusted website when in fact the browser opens a malicious website.

The weakness has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2.

References:
http://secunia.com/advisories/17565/

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