netVigilance

ScoutNews Team **26 November 2004**
Issue #48

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

We may very well become witnesses to one of weirdest commercial moves ever if TiVo who controls its customer environment 100% moves forward with enabling pop-up ads.
We are still in limbo where there is no one cure all solution for the digital security market, wile it has been long coming for the FBI to go to one of the most obvious sources for tracking criminals; www.insecure.org .

Enjoy reading

Top Security News Stories this Week

- **TiVo Pop-Up Ads Raise Consumer Concerns**

  Digital video recording pioneer TiVo (news - web sites) Inc. has long promised "TV Your Way." But the company's plans for pop-up ads and restrictions on copying have sparked worries that the service may be eroding consumer control in favor of Hollywood and advertiser interests.
  Is it becoming TiVo — their way? "Consumers are very distrustful of technologies that seize yet another opportunity to offer up advertising," said Mike Godwin, legal director of Public Knowledge, a public interest group. Whether the fears are founded or not, he said, "it feels like TiVo is taking away some of the prerogatives and flexibility that TiVo TV watchers have become accustomed to."
  http://story.news.yahoo.com/news?tmpl=story&cid=562&ncid=738&e=2&u=/ap/20041126/ap_on_hi_te/tivo_surrender

  May Wong

- **Online Identity Theft: Many Medicines, No Cure**

  As the incidence of online identity theft has steadily climbed in recent months, banks and online retailers have struggled to stay on top of the problem and to protect their customers, whose personal financial information and online account details are coveted by criminals. But as problems like phishing scams change from e-crime phenomenon to endemic online threats, technology companies--both large and small--are bringing products and services to market that they claim can end, or greatly reduce, the threat of online identity theft.
  http://story.news.yahoo.com/news?tmpl=story&ncid=1212&e=8&u=/pcworld/20041126/tc_pcworld/118709&sid=95612658

  Paul Roberts

- **Hacking tool 'draws FBI subpoenas'**

The author of the popular freeware hacking tool Nmap warned users this week that FBI agents are increasingly seeking access to information from the server logs of his download site, insecure.org.
"I may be forced by law to comply with legal, properly served subpoenas," wrote "Fyodor," the 27-year-old Silicon Valley coder responsible for the post scanning tool, in a mailing list message. "At the same time, I'll try to fight anything too broad... Protecting your privacy is important to me, but Nmap users should be savvy enough to know that all of your network activity leave traces."
http://www.theregister.co.uk/2004/11/25/nmap_draws_fbi_subpoenas/
Keven Paulsen

New Vulnerabilities Tested in SecureScout

- **15134 Winamp "IN_CDDA.dll" Buffer Overflow Vulnerability (Remote File Checking)**

  The Winamp Player is a flexible and sophisticated application for playing and managing music.

  The vulnerability is caused due to a boundary error in the "IN_CDDA.dll" file. This can be exploited in various ways to cause a stack-based buffer overflow e.g. by tricking a user into visiting a malicious web site containing a specially crafted ".m3u" playlist. Successful exploitation allows execution of arbitrary code.
  The vulnerability has been reported in version 5.05 and confirmed in version 5.06. Prior versions may also be affected.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://www.winamp.com/ & http://www.security-assessment.com/Papers/Winamp_IN_CDDA_Buffer_Overflow.pdf

- **15537 IOS Reload after Scanning Vulnerability (CSCds07326)**

  Security Scanning software can cause a memory error in Cisco IOS® Software that will cause a reload to occur.
  The security scanner makes TCP connection attempts to various ports, looking for open ports to further investigate known vulnerabilities with those services associated with certain ports. However, a side effect of the tests exposes the defect described in this security advisory, and the router will reload unexpectedly as soon as it receives a request to review or write the configuration file.

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

CVE Links: CVE-2001-0750

Reference:
http://www.cisco.com/en/US/products/products_security_advisory09186a00800b13b2.shtml

❖ **15538 Cisco Catalyst Memory Leak Vulnerability (CSCds66191)**
A series of failed telnet authentication attempts to the switch can cause the Catalyst Switch to fail to pass traffic or accept management connections until the system is rebooted or a power cycle is performed. All types of telnet authentication are affected, including Kerberized telnet, and AAA authentication.

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

CVE Links: CVE-2001-0041

Reference:
http://www.cisco.com/en/US/products/products_security_advisory09186a00800b138e.shtml

❖ **15539 Cisco IOS PPTP Vulnerability (CSCdt46181)**
PPTP implementation using Cisco IOS® software releases contains a vulnerability that will crash a router if it receives a malformed or crafted PPTP packet. To expose this vulnerability, PPTP must be enabled on the router. PPTP is disabled by default. No additional special conditions are required

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

CVE Link: CVE-1999-0162

Reference:
http://www.cisco.com/en/US/tech/tk827/tk369/technologies_security_advisory09186a00800b1695.shtml

❖ **15540 Cisco VPN 3000 Concentrator Multiple Vulnerabilities (CSCdt56514)**
The Cisco VPN 3000 series concentrators are a family of purpose-built, remote access Virtual Private Network (VPN) platforms for data encryption and authentication.

Test Case Impact: **Gather info** Vulnerability Impact: **Attack** Risk: **High**

CVE Link: CAN-2002-1092 & CAN-2002-1095

Reference:
http://www.cisco.com/en/US/products/products_security_advisory09186a00800c8154.shtml

❖ **15541 Catalyst 5000 Series 802.1x Vulnerability (CSCdt62732)**
This vulnerability affects the following Catalyst models 5000, 5002, 5500, 5505, 5509, 2901, 2902 and 2926 switches.

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

CVE Link: CVE-2001-0429

Reference:
http://www.cisco.com/en/US/products/products_security_advisory09186a00800b138d.

❖ **15542 Cisco 6400 NRP2 Telnet Vulnerability (CSCdt65960)**
The Cisco 6400 Access Concentrator Node Route Processor 2 (NRP2) module allows

Telnet access when no password has been set.

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

CVE Link: CVE-2001-0757

Reference:
http://www.cisco.com/en/US/products/products_security_advisory09186a00800b1388.shtml

- **15543 Cisco VPN 3000 Concentrator Multiple Vulnerabilities (CSCdu15622)**
  The Cisco VPN 3000 series concentrators are a family of purpose-built, remote access Virtual Private Network (VPN) platforms for data encryption and authentication.

Test Case Impact: **Attack** Vulnerability Impact: **DoS** Risk: **High**

CVE Link: CAN-2002-1092 & CAN-2002-1095

Reference:
http://www.cisco.com/en/US/products/products_security_advisory09186a00800c8154.shtml

- **15544 Data Leak with Cisco Express Forwarding Enabled (CSCdu20643)**
  Excluding Cisco 12000 Series Internet Routers, all Cisco devices running Cisco IOS® software that have Cisco Express Forwarding (CEF) enabled can leak information from previous packets that have been handled by the device.

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

CVE Link: CVE-2002-0339

Reference:
http://www.cisco.com/en/US/tech/tk827/tk831/technologies_security_advisory09186a0080094716.shtml

- **15545 Cisco VPN 3000 Concentrator Multiple Vulnerabilities (CSCdu35577)**
  The Cisco VPN 3000 series concentrators are a family of purpose-built, remote access Virtual Private Network (VPN) platforms for data encryption and authentication.

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

CVE Link: CAN-2002-1094

Reference: http://www.cisco.com/warp/public/707/vpn3k-multiple-vuln-pub.shtml

New Vulnerabilities found this Week

- **Winamp "IN_CDDA.dll" Buffer Overflow Vulnerability**
  “Execution of arbitrary code”
  Brett Moore has reported a vulnerability in Winamp, which can be exploited by malicious people to compromise a user's system.
  The vulnerability is caused due to a boundary error in the "IN_CDDA.dll" file. This can

be exploited in various ways to cause a stack-based buffer overflow e.g. by tricking a user into visiting a malicious web site containing a specially crafted ".m3u" playlist.
Successful exploitation allows execution of arbitrary code.
The vulnerability has been reported in version 5.05 and confirmed in version 5.06. Prior versions may also be affected.
References:
http://www.security-assessment.c...namp_IN_CDDA_Buffer_Overflow.pdf

❖ **Linux Kernel Local DoS and Memory Content Disclosure Vulnerabilities**

"Denial of Service"
Two vulnerabilities have been reported in the Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service) or gain knowledge of potentially sensitive information.
1) An unspecified error can be exploited via a specially crafted a.out binary to cause a DoS.
2) A race condition within the memory management can be exploited to disclose the content of random physical memory pages.
References:
http://www.suse.de/de/security/2004_01_sr.html

❖ **SecureCRT Arbitrary Configuration Folder Specification Vulnerability**

"Execution of arbitrary commands"
Brett Moore has reported a vulnerability in SecureCRT, which can be exploited by malicious people to compromise a user's system.
The vulnerability is caused due to a design error, as the product allows an arbitrary configuration folder to be specified to the "telnet:" URI handler via the "/F" command line option.
This can e.g. be exploited by including a link to a remote configuration folder on a SMB share and trick a user into visiting a malicious web site containing the link.
Successful exploitation allows execution of arbitrary commands via a malicious logon script with the privileges of the user running SecureCRT.
The vulnerability has been reported in versions 4.1 and 4.0. Prior versions may also be affected.
References:
http://www.security-assessment.c...CRT_Remote_Command_Execution.pdf

❖ **Cyrus IMAP Server Multiple Vulnerabilities**

"Execution of arbitrary code"
Stefan Esser has reported four vulnerabilities in Cyrus IMAP Server, which can be exploited by malicious people to compromise a vulnerable system.
1) A boundary error within the handling of the "PROXY" and "LOGIN" commands can be exploited to cause a stack-based buffer overflow by passing an overly long username.
Successful exploitation allows execution of arbitrary code prior to authentication, but requires that the "IMAPMAGICPLUS" option is enabled.
This vulnerability has been reported in versions 2.2.4 through 2.2.8.
2) An input validation error within the argument parser for the "PARTIAL" command can be exploited to reference memory outside an allocated buffer.
Combined with another error, successful exploitation allows overwriting a single byte, which may allow execution of arbitrary code.
This vulnerability has been reported in version 2.2.6 and prior.

3) An input validation error within the argument handler for the "FETCH" command can be exploited to reference memory outside an allocated buffer.
Combined with another error, successful exploitation allows overwriting a single byte, which may allow execution of arbitrary code.
This vulnerability has been reported in version 2.2.8 and prior.
4) The handler for the "APPEND" command uses an undefined programming construct, which potentially could result in an attacker-supplied pointer being freed.
Successful exploitation may potentially allow execution of arbitrary code.
This vulnerability has been reported in versions 2.2.7 and 2.2.8.
References:
http://security.e-matters.de/advisories/152004.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