netVigilance

SecureNews Team **2 January 2004**
Issue #1

Weekly SecureNews by netVigilance

Table of Contents

Welcome to the New Year – Good Luck

Happy New Year!
Most of us have been busy coping with the everyday churn of IT security issues that come along at increasing speed. The New Year is on us and a lot of people are forecasting what will be happening in the IT security field during 2004.
Well, some trends will not change – the continuous stream of vulnerabilities and related exploits is here and will still be here a year from now.
We will see more worms with dangerous nature in 2004 and organizations will need to be even more diligent in managing their infrastructures.
The probability of a so-called “Zero day” attack is real; however the real threat still sits with known issues, disgruntled employees and organized crime.
Regulations will continue kicking in and we will see more structured criminal forensics targeted at hackers, organized crime and other unlawful individuals.
2004 will be the year where proactive security achieves a level of acceptance and understanding that it will become possible to start standardizing it, this is important as it is what needs to happen to reverse the cycle of the good guy reacting to what the bad guy does.
So… here is our look into the crystal ball for IT security products in 2004:

1. Convergence of discrete security applications into integrated security solutions; expect to see testing, patching, correlation, security management and other functionality melt together.
2. Real time hardware assisted content inspection will be the key for edge security appliances and will change the competitive landscape within the firewall, IDS and antivirus segments.
3. Behavioral based security policies will be the hot thing in switching infrastructure as a pre-curser to the standardized layer 3-7 security that will arrive in 2005 or 2006

- Good luck.

New Vulnerabilities Tested for in SecureScout

(These test cases will be available as of Monday January 5th)

- **11023 Cisco IOS ICMP Redirect Denial Of Service Vulnerability**

IOS is the Internet Operating System, used on Cisco routers. It is distributed and maintained by Cisco. It has been reported that it is possible to cause a denial of service in some Cisco routers by sending a large amount of spoofed ICMP redirect messages. Bottom line: A remote attacker can compromise your Cisco device and thus prevent you legitimate users from accessing your network.

Test Case Impact: **Denial of Service** Vulnerability Impact: **Gather Info** Risk: **High**

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1222
Initial Advisory: http://www.phenoelit.de/stuff/CiscoICMP.txt
Securityfocus.com : http://online.securityfocus.com/archive/1/273421
Cisco Bug ID: CSCdx32056
http://www.cisco.com/warp/public/770/fn23074.shtml
See also: http://www.securityfocus.com/bid/4786
Product Page: http://www.cisco.com
http://home.t-online.de/home/theRealCoders/smurf/index.html

- **15480 Cisco IOS UDP Echo Service Memory Disclosure Vulnerability**

With this vulnerability it is possible to disclose sensitive memory information by sending crafted packets to your Cisco routers. Cisco IOS is the running on Cisco routers. If the udp-small-servers command is enabled, a Cisco IOS® software device may reply to malformed udp echo packets with some of the contents stored in a router's memory. By repeatedly sending malformed udp echo packets and capturing the replies, an attacker can obtain portions of the data that is stored in a router's memory. Workarounds are available to mitigate the effects.

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

CVE Link: No CVE link available
Bugtraq: http://www.securityfocus.com/advisories/5659
BID: http://www.securityfocus.com/bid/8323
http://www.secunia.com/advisories/9414
Cisco advisory: http://www.cisco.com/warp/public/707/cisco-sn-20030731-ios-udp-echo.shtml

- **17700 Arbitrary file Disclosure (Directory Traversal / File Truncation) for SAP Internet Transaction Server**

This vulnerability allows remote attackers to access to arbitrary file (Directory Traversal / File Truncation). Due to truncation on input values if they exceed a given length, it's possible to shed the ".html" extension in wgate.dll for SAP Internet Transcaction Server (ITS) 4620.2.0.323011 that allows remote attackers to access to arbitrary file (Directory Traversal / File Truncation).

Test Case Impact: **Attack** Vulnerability Impact: **Root Gain** Risk: **Medium**

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0749
BUGTRAQ: 20030830 SAP Internet Transaction Server
URL: http://archives.neohapsis.com/archives/bugtraq/2003-08/0361.html
http://www.securityfocus.com/archive/1/335593

- **17702 Cross-site Scripting (XSS) Vulnerability for SAP Internet Transaction Server**

  This vulnerability allows remote attackers to insert arbitrary web script and steal cookies. Cross-site scripting (XSS) vulnerability in wgate.dll for SAP Internet Transcaction Server (ITS) 4620.2.0.323011 allows remote attackers to insert arbitrary web script and steal cookies via the ~service parameter.

  Test Case Impact: **Attack** Vulnerability Impact: **Attack** Risk: **Medium**

  CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0749
  BUGTRAQ:20030830 SAP Internet Transaction Server
  URL: http://archives.neohapsis.com/archives/bugtraq/2003-08/0361.html
  http://www.securityfocus.com/archive/1/335593

Top Security News Stories this Week

- **Security Predictions For 2004**
  Top 10 lists are everywhere. This one by Peter Gregory of ComputerWorld is pretty good, but you will find links to other pundants below. If you are not already hip deep in these issues, you will be soon enough if you have the technology deployed. In 2004, information security professionals will experience more of the darker side of human behavior, but organizations will also take more control over their network and computing infrastructures, particularly end-user systems. Finally, the 2004 presidential election will continue to focus public and media attention on the security of embedded operating systems in everything from electronic voting kiosks to ATMs, experts say. Security flaws, the increasing use of embedded versions of Windows, and the near-total dominance of the TCP/IP networking protocol make it likely virus and worm outbreaks will affect private networks used by ATMs, utilities, and other critical systems, even if those systems don't run Windows. Here are a few predictions on what to expect in information security in the next year along with an insightful article posted on TechWeb.
  http://www.computerworld.com/securitytopics/security/story/0,10801,88113,00.html
  http://www.pcworld.com/news/article/0,aid,114058,00.asp
  http://www.vnunet.com/News/1151740
  http://www.techweb.com/wire/story/TWB20031229S0006
  By ComputerWorld – Peter Gregory / Gregg Keizer – Tech Web / Ian Thomson – vnunet / Paul Roberts - IDG

- **The 2003 Virus Hall of Fame**
  It's hard to resist the hall of fame game this time of year. This year was marked by periods of relative quiet and then intense hacking activities. August was the worst month for viruses in IT history. Read Help Net's top virus list as well as their retrospective on Wireless security issues. Below are a few of the more notable viruses that attacked our networks last year. May they not return anytime soon.
  - The most damaging virus: for two reasons this goes to Bugbear.B.
  - The most effective virus: SQLSlammer is hard to beat in this category.
  - The most persistent virus: Klez.I wins hands down.
  - The most ingenious virus: in this category, Gibe.C stands out on its own.
  - The most annoying virus: this award goes to Blaster
  - The most cunning virus: Nachi.A

- The most opportunist: Ganda.A. Sneaky. Posed as satellite photos of recent hostilities.

http://www.net-security.org/article.php?id=622
By Berislav Kucan – Help Net Security

❖ **PowerPoint Vs. Clarity and Specificity**
A few weeks back, we ran a story about NASA's problems with PowerPoint presentations glossing over the details. Ironically, the best antidote to PowerPoint may be a guide to technical writing that was published by NASA many years ago, and can still be downloaded from NASA's own servers:
http://techreports.larc.nasa.gov/ltrs/1964-cit.html That page is a link to this file: http://techreports.larc.nasa.gov/ltrs/PDF/NASA-64-sp7010.pdf "Clarity in Technical Reporting" by S. Katzoff was written in 1955 and circulated informally at NASA's Langley Research Center. Popular demand led NASA to publish it officially in 1964. The PDF file on the web is a scan of a copy that was printed in 1973. The first 16 pages are about written reports, the last 9 pages are about verbal presentations. The author assumes that the slides will be charts and graphs, not bullet points.
http://catless.ncl.ac.uk/go/risks/23/10/10
By Ron Bean – shell.core

❖ **Defenses Lacking At Social Network Sites**
Services like LiveJournal and Tribe are poised to be the next big thing on the Web in 2004, but their security and privacy practices are more like 1997. Brad Fitzpatrick is president of LiveJournal.com, a social discovery Web site where over 1.5 million users post diary entries they want to share with friends. Although members post extremely sensitive information in their journals -- everything from their plans to commit suicide or sabotage their boss to their latest sexual adventures -- Fitzpatrick admits that security on his site isn't a priority.
http://www.securityfocus.com/news/7739
By Annalee Newitz – Security Focus

❖ **Defenses Electronic Voting Firm's Site Hacked**
you've already read a lot about hacking of electronic voting systems. And with the technology just becoming widespread, you will read a lot more in the future. As the year drew to an end, a company developing security technology for electronic voting suffered an embarrassing hacker break-in that executives think was tied to the rancorous debate over the safety of casting ballots online. VoteHere Inc. of Bellevue, Wash., confirmed Monday that U.S. authorities are investigating a break-in of its computers months ago, when someone roamed its internal computer network. The intruder accessed internal documents and may have copied sensitive software blueprints that the company planned eventually to disclose publicly.
http://www.extremetech.com/article2/0,3973,1424878,00.asp
By Ted Brindis – AP Tech writer

New Vulnerabilities this Week

PHPCatalog ID Parameter SQL Injection Vulnerability

A vulnerability has been reported to exist in PHPCatalog that may allow a remote user to inject malicious SQL syntax into database queries. The problem reportedly exists in the URI parameters of PHPCatalog. This issue is caused by insufficient sanitization of user-supplied

data. A remote attacker may exploit this issue to influence SQL query logic to have unauthorized SQL queries executed in the database.
For more information, see http://www.securityfocus.com/bid/9318/discussion/
Source: Security Focus

WorldClient Form2Raw Raw Message Handler Buffer Overflow Vulnerability
It has been reported that MDaemon/WorldClient mail server may be prone to a buffer overflow vulnerability when handling certain messages with a 'From' field of over 249 bytes. This issue may allow a remote attacker to gain unauthorized access to a system. Successful exploitation of this issue may allow an attacker to execute arbitrary code in the context of the vulnerable software in order to gain unauthorized access.
For more information, see http://www.securityfocus.com/bid/9317/discussion/
Source: Security Focus

Microsoft IIS Failure to Log Undocumented TRACK Requests Vulnerability
A vulnerability has been reported to affect Microsoft IIS. It has been reported that IIS fails to log HTTP TRACK calls made to the affected server. A remote attacker may exploit this condition in order to enumerate server banners.
For more information, see http://www.securityfocus.com/bid/9313
Source: SecurityFocus

Microsoft Internet Explorer showHelp() '\..\' Directory Traversal Flaw Lets Remote Users Execute Files on the Target System
A vulnerability was reported in Microsoft Internet Explorer in the showHelp() function. A remote user can execute arbitrary files on the target system. A remote user can create HTML that exploits a directory traversal flaw in the showHelp() implementation to execute arbitrary specified 'chm' files on the target system. The files will run in the Local Computer security zone with the privileges of the target user.
For more information, see http://www.securitytracker.com/alerts/2003/Dec/1008578.html
Security Tacker

SANS Latest List of Security Vulnerabilities
(1) HIGH: ALT-N MDaemon Raw Message Handler Buffer Overflow
(2) HIGH: NetObserve Authentication Bypass Vulnerability
(3) HIGH: Knowledge Builder PHP Remote File Include Vulnerability
(4) MODERATE: LANDesk IRCRBOOT.DLL ActiveX Control Buffer Overflow
(5) MODERATE: Platinum FTP Server Format String Vulnerabilities
(6) MODERATE: Xlight FTP Server Password Buffer Overflow
(7) MODERATE: Jordan Windows Telnet Server Buffer Overflow
(8) LOW: Surfboard HTTP Server Buffer Overflow
For more information, see http://www.sans.org/newsletters/risk/vol2_53.php
Source: SANS

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 SecureNews. 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 SecureNews@netVigilance.com.