netVigilance

SecureNews Team **9 January 2004**
Issue #2

Weekly SecureScout News by netVigilance

Table of Contents

New Vulnerabilities Tested for in SecureScout

- **14195 Password Cannot Change Vulnerability**

  A Windows account policy for passwords has inappropriate, security-critical settings. The user has a password that does not change. If this is a service account, then this condition does not indicate vulnerability.

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

  CVE Link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0535

- **14377 Cumulative Security Update for Internet Explorer (MS03-048/824145) Vulnerability**

  This is a cumulative update that incorporates the functionality of all previously released updates for Internet Explorer. Additionally, this update eliminates the following newly reported vulnerabilities: Three vulnerabilities that could allow an attacker to cause arbitrary code to run on the user's system. A vulnerability that could allow an attacker to access local files and cookies on a user's system. A vulnerability that could allow an attacker to save arbitrary code on the user's system.

  Test Case Impact: **Gather Info** Vulnerability Impact: **Gain Root** Risk: **High**

  CVE Links: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0814
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0815
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0816
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0817
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0823
  Initial Advisory: http://www.microsoft.com/technet/security/bulletin/MS03-048.asp

- **14380 Cumulative Patch for Internet Explorer (MS03-040/828750) Vulnerability**

  A vulnerability occurs because Internet Explorer does not properly determine an object type returned from a Web server in a popup window. It could be possible for an attacker who exploited this vulnerability to run arbitrary code on a user's system. If a user visited an attacker's Web site, it could

be possible for the attacker to exploit this vulnerability without any other user action. An attacker could also craft an HTML–based e-mail that would attempt to exploit this vulnerability.

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

CVE Links: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0838
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0809
Initial Advisory: http://www.microsoft.com/technet/security/bulletin/MS03-040.asp

- **14383 Buffer Overflow in the Windows Troubleshooter ActiveX Control Could Allow Code Execution Vulnerability**

A security vulnerability exists in the Microsoft Local Troubleshooter ActiveX control. The vulnerability exists because the ActiveX control contains a buffer overflow that could allow an attacker to run code of their choice on a user's system. Because this control is marked "safe for scripting", an attacker could exploit this vulnerability by convincing a user to view a specially crafted HTML page that references this ActiveX control. The Microsoft Local Troubleshooter ActiveX control is installed as a default part of the operating system on Windows 2000.

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

CVE Link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0662
Microsoft Link: http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-042.asp

- **14384 Buffer Overrun in the ListBox and in the ComboBox Control Could Allow Code Execution Vulnerability**

A vulnerability exists because the ListBox control and the ComboBox control both call a function, which is located in the User32.dll file, that contains a buffer overrun. The function does not correctly validate the parameters that are sent from a specially-crafted Windows message. Windows messages provide a way for interactive processes to react to user events (for example, keystrokes or mouse movements) and to communicate with other interactive processes. A security vulnerability exists because the function that provides the list of accessibility options to the user does not correctly validate Windows messages that are sent to it. One process in the interactive desktop could use a specific Windows message to cause the ListBox control or the ComboBox control to execute arbitrary code. Any program that implements the ListBox control or the ComboBox control could allow code to be executed at an elevated level of administrative credentials, as long as the program is running at an elevated level of privileges (for example, Utility Manager in Windows 2000). This could include third-party applications.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gain Root** Risk: **High**

CVE Link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0659
Microsoft Link: http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-045.asp
Security Focus: http://securityfocus.com/bid/8827

- **15484 Multiple Cisco PIX Remote Denial Of Service Vulnerabilities**

  This vulnerability can be exploited to initiate a Denial of Service attack on the Cisco FWSM. The Cisco FWSM crashes and reloads while processing a received SNMPv3 message when snmp-server host <if_name> <ip_addr> or snmp-server host <if_name> <ip_addr> poll is configured on the Cisco FWSM. This happens even though the Cisco FWSM does not support SNMPv3. A Cisco FWSM configured to only generate and send traps using the snmp-server host <if_name> <ip_addr> trap command is not vulnerable. Under certain conditions, an established VPNC IPSec tunnel connection is dropped if another IPSec client attempts to initiate an IKE "Phase I" negotiation to the outside interface of the VPN Client configured Cisco PIX firewall. Only a Cisco PIX firewall configured as a VPN Client is vulnerable to this vulnerability.

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

  CVE Link: No CVE link available
  Security Focus: http://www.securityfocus.com/bid/9221/
  Cisco: http://www.cisco.com/warp/public/707/cisco-sa-20031215-fwsm.shtml
  Security Team: http://www.securiteam.com/securitynews/6D00E2A96W.html

- **15503 SurfControl Email Filter for SMTP HELO Denial of Service Vulnerability**

  SurfControl SuperScout Email filter for SMTP 3.5.1 is reportedly vulnerable to a denial of service attack (and possible buffer overflow). This is possible by connecting to the SMTP service and sending HELO with an excessively long argument (greater than 905 characters). If the software is set to automatically restart, SMTP and filtering services will resume once this has happened. Other SMTP commands may also be used to initiate this condition.

  Test Case Impact: **Denial of Service** Vulnerability Impact: **Denial of Service** Risk: **Low**

  CVE Link: No CVE link available
  BID: http://www.securityfocus.com/bid/4257
  Product Page: http://www.surfcontrol.com/

- **15505 Sendmail Long Ident Logging Circumvention Weakness Vulnerability**

  A remote attacker can compromise your mail server by misleading you with bad server information. Sendmail is a freely available, open source mail transport agent. It is maintained and distributed by the Sendmail Consortium. It has been reported that Sendmail does not properly handle long idents. Due to the improper handling of long idents, an attacker may supply a long ident which will result in the omission of the IP address from logs when a user attempts certain commands.

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

  CVE Link: No CVE Link available
  Initial Advisory: http://online.securityfocus.com/archive/1/292779
  See also: http://www.securityfocus.com/bid/5770
  Product Page: http://www.sendmail.org/

- **17396 Cisco VPN 3000 Concentrators Maxlength in Admin Page DoS Vulnerability**

  It is possible for a remote user to send malicious packets to a VPN 3000 Concentrator, and deny service to legitimate users of network resources. Cisco VPN 3000 series concentrators allow by submitting malicious specially crafted packets to their webserver to perform a denial of service. This is due to CGI script lacking of input sanitizing. This should force a reboot of the host.

  Test Case Impact: **Crash** Vulnerability Impact: **Crash** Risk: **High**

  CVE Link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1100
  Cisco Advisory: http://www.cisco.com/warp/public/707/vpn3k-multiple-vuln-pub.shtml
  VIGILANTe Advisory: http://www.vigilante.com/inetsecurity/advisories/VIGILANTE-2002002.htm
  BID: http://online.securityfocus.com/bid/5617

- **17800 wu-ftpd Debug Mode Client Hostname Format String Vulnerability**

  It is possible to run arbitrary commands on your host by sending crafted packets to your FTP server. wu-ftpd is a very popular FTP server. A format string class vulnerability in wu-ftp 2.6.1 and earlier, when running with debug mode enabled, allows remote attackers to execute arbitrary commands via a malformed argument that is recorded in a PASV port assignment.

  Test Case Impact: **Gather Info** Vulnerability Impact: **Gain Root** Risk: **High**

  CVE Link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0187
  CERT: http://www.kb.cert.org/vuls/id/639760
  BID: http://www.securityfocus.com/bid/2296
  Product page: http://www.wu-ftpd.org/
  October 2002 SANS Top 20: http://www.sans.org/top20/oct02.php

Top Security News Stories this Week

- **Trojan Poses as Windows XP Update**

  A new Swen-style Trojan horse posing as a critical update from Microsoft has been detected on the Internet. Users who open the e-mail message may find their machines loaded with a back-door Trojan that can steal passwords or be used in conjunction with other systems to conduct major denial-of-service (DoS) attacks. Dubbed Trojan.Xombe (as in zombie) by most security firms, the Trojan shares some characteristics of the Swen worm family in that it masquerades as a message from Microsoft and purports to carry a security update in its file attachment. However, unlike Swen -- a worm which first appeared last September -- Trojan.Xombe doesn't self-replicate. The program arrives as an executable attachment in spam e-mail messages purporting to come from windowsupdate@microsoft.com and installs itself on victim's computers when users open the attachment. Once installed, Xombe connects to a Web site, then downloads and installs another program, called Mssvc-A, which is a Trojan Horse program that conscripts victim computers in distributed denial of service attacks against Web pages, according to antivirus company Sophos. Xombe is considered a low risk by most antivirus companies, including Sophos, Computer Associates International, and Symantec. The program is not a worm or virus and cannot make copies of itself. Instead, it is distributed using spam e-mail messages.

http://www.pcworld.com/news/article/0,aid,114237,00.asp
http://www.techweb.com/wire/story/TWB20040109S0009
By Paul Roberts – IDG News / Gregg Keizer - TechWeb

❖ **Microsoft's Narrowband Security Hurdle**

Microsoft's recent release of a scaled-down removal tool for the MSBlaster worm was an unprecedented move aimed at reaching an elusive element of the destructive worm: home and small business PC users. As part of its bid to reach dial-up subscribers who haven't bothered to download a patch that removes the worm, the software giant's security unit stripped out as much as they could from the tool in order to make the patch a faster download. The scaled-down approach illustrates a persistent problem in patch-management: how to load the patches on home users' PCs.

http://www.internetnews.com/infra/article.php/3297651
By Ryan Narine - Internet News

❖ **Top Networking Technologies for 2004**

Read the NewsFactor Intel interview about what is coming for networking in 2004. The list includs putting wireless behind the corporate firewall, scalable servers, blade servers, global services assessment, speech-based servers and more. According to Tim Dunn, the buildout of next-generation I.T. networks during 2004 will be dominated by the move to place technologies behind corporate firewalls, as well as the switch to new servers in various scalable and high-density iterations. "Wireless will ultimately penetrate everything we do, as well as change how corporate users work," says Tim Dunn, chief technology officer for Intel Communications Group. The introduction of wireless behind the corporate firewall will even enhance network security.

http://www.newsfactor.com/story.xhtml?story_title=Top_Networking_Technologies_for_____&story_id=22968&category=netsecurity
By Mark Long – News Factor

❖ **Flaws Raise Red Flag on Linux Security**

ComputerWorld reported last week about a critical flaw in the Linux kernel was the latest in a series of recently discovered security problems with the popular open-source operating system. But many users were unfazed by the report and said Linux remains a solid and secure environment for running enterprise applications. Poland-based iSec Security Research on Monday said it had found a critical flaw in a function used to manage virtual memory on Linux systems (see story). The flaw affects the 2.2, 2.4 and 2.6 versions of the Linux kernel, according to iSec. The vulnerability could allow attackers to take administrative control of compromised systems and run attack code of their choice, an iSec advisory stated. ISec claimed that it had developed and successfully tested code that was capable of exploiting the flaw, although it added that actually launching such an attack wouldn't be easy.

http://www.computerworld.com/softwaretopics/os/linux/story/0,10801,88936,00.html
By Jaikumar Vijayan - ComputerWorld

❖ **Linux Security Auditing Tool Released**

Linux Security Auditing Tool (LSAT) is a post install security auditing tool. It is modular in design, so new features can be added quickly. It checks many system configurations and local network

settings on the system for common security/config errors and for packages that are not needed. It has been tested on Linux (Gentoo, Red Hat, Debian, etc.) and Solaris (SunOS 2.x).

http://freshmeat.net/projects/lsat/?branch_id=28349&release_id=147443&topic_id=253
By Triode – Freshmeat.net

- **VeriSign Dead Cert Causes Net Instability**

The expiration of one of VeriSign's master digital certificates on Wednesday created confusion for Net users and glitches to the operation of some applications, notably Norton Anti-Virus (NAV). After the cert VeriSign used to sign other certs expired, the chain of trust was broken, leaving some aps unable to set up a secure connection. These apps then defaulted to trying to access Verisign's certificate revocation list server (crl.verisign.com) which, faced with a huge extra load, buckled under the pressure. Verisign has posted an advisory on the problem here, detailing server updates needed to resolve application instability. Essentially where there are problems traffic needs to be directed to a new Global Server Intermediate Root CA. Users of Java aps and older IE browsers were affected by the issue but (judging by our postbag) NAV users were worst affected. NAV Users saw their computers slow to a crawl and Microsoft office apps not starting properly because of the problem.

http://www.theregister.co.uk/content/55/34801.html
By John Leyden – The Register

New Vulnerabilities this Week

Windows FTP Server Format String Vulnerability
A highly critical vulnerability has been reported in Windows Ftp Server, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system. The vulnerability is caused due to a format string error when processing client data. This can e.g. be exploited by supplying a specially crafted username containing format specifiers when attempting to log in. Successful exploitation may crash the process or potentially allow execution of arbitrary code. The vulnerability has been reported in version 1.6 and prior.
For more information, see http://www.secunia.com/advisories/10589/
Source: Secunia

phpGroupWare Flaws Allow SQL Injection and PHP File Uploading
Some vulnerabilities were reported in phpGroupWare. A remote user may be able to inject SQL commands. A remote authenticated user may be able to upload PHP scripts and execute them on the target server. It is reported that the 'calendar' and 'infolog' modules do not properly escape user-supplied input. A remote user may be able to supply a specially crafted request to execute SQL queries on the underlying database. It is also reported that the 'calendar' module allows a remote authenticated user to upload holiday files containing PHP code that can later be remotely executed. The 'save extension' is reportedly not properly enforced. The PHP code will execute with the privileges of the target web service.
For more information, see http://www.securitytracker.com/alerts/2004/Jan/1008662.html
Source: Security Tracker

PhpGedView Multiple PHP Remote File Include Vulnerabilities
PhpGedView is prone to multiple file include vulnerabilities. The source of the issue is that a number of scripts that ship with the software permit remote users to influence require() paths for various external

files. This will permit remote attackers to cause malicious PHP scripts from attacker-controlled servers to be included and subsequently executed in the context of the web server hosting the vulnerable software.
For more information, see http://www.securityfocus.com/bid/9368/discussion/
Source: Security Focus

Jabber Server SSL Handling Denial of Service Vulnerability
It has been reported that the Jabber server is vulnerable to a remotely exploitable denial of service condition. The flaw that can trigger the condition is allegedly due to a failure to handle certain types of SSL connections. Remote attackers may exploit this vulnerability to cause the server to crash, resulting in a denial of service.
For more information, see http://www.securityfocus.com/bid/9376
Source: Security Focus

Spoofed Kernel Netlink Interface Message Denial of Service Vulnerability
Applications which make use of the kernel Netlink interface are said to be prone to denial of service attacks. It has been reported that applications implementing the getifaddrs() glibc function may be prone to denial of service attacks. The problem is said to occur due to the way getifaddrs() interacts with the netlink device. Under some circumstances, an anonymous netlink message handled by the getifaddrs() function may cause the application to crash. Red Hat has stated that GNU Zebra, Quagga and iproute are also affected by this vulnerability due to the way they interact with the netlink interface; exploitation may result in a denial of service.
For more information, see http://www.securityfocus.com/bid/9027
Source: Security Focus

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.