netVigilance

ScoutNews Team **16 April 2004**
Issue #16

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Bill Gates is vowing to put even more effort into security.

Worms can do it all by them selves now – even as major security equipment vendors are starting to quarantine or arrest mails so they don't arrive at users workstations; the worms don't need the ignorance of a user to get started any more.
Again: This is why you need to perform in-line on-going vulnerability assessment and mitigation. In short this is Vulnerability Management.

Now the large facilities at universities are being addressed by the people on the dark side; this is probably good seen from a US biased homeland security effort as these very open and easy to access networks now will get the attention they need and hopefully become more secure for our global society.

Enjoy reading

Top Security News Stories this Week

- **Microsoft to invest more in security: Bill Gates**
  Malicious software code has been around for decades. But only in the last few years have the Internet, high-speed connections and millions of new computing devices converged to create a truly global computing network in which a virus or worm can circle the world in a matter of minutes.
  http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/56042751?-2622
  Bill Gates

- **Netsky-V worm can infect computers without e-mail attachment being clicked**
  No need to double-click to be infected by Netsky-V the new Netsky-V worm (W32/Netsky-V) spreads without using email attachments to infect. Other widespread versions of the Netsky worm have infected users by tempting them to double-click on an email attachment, but Netsky-V exploits security loopholes in Microsoft's software that mean users can be hit just by reading an email. Emails containing the exploit, which can use subject lines such as 'Converting message. Please wait...' and 'Please wait while

loading failed message...', attempt to download a copy of the worm from another user's computer. "Home users are especially vulnerable to this kind of attack as their computers are often not properly protected with a personal firewall or the latest anti-virus updates," said Graham Cluley, senior technology consultant for Sophos. "Personal computer users should consider checking out Microsoft's security update website, which can scan home PCs for security vulnerabilities and suggest which critical patches need to be installed."
http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?database=JanEE%2edb&command=viewone&id=10&op=t
from the folks at Sophos

DHS, DOD disagree on cybersecurity and secrecy
Keeping secrets and bare-bones budgets dominated a discussion of federal cybersecurity research this week at a meeting of the President's Information Technology Advisory Committee.
Secrecy has become an issue because federal agencies that provide research funds for cybersecurity are split over whether research results should be classified. Defense Advanced Research Projects Agency officials who spoke at the meeting said they consider most of the agency's cybersecurity research to be classified information
http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/56038376?-2622
Florence Olsen

- **Hackers hit US universities**
  HACKERS have broken into some of the world's most powerful computer clusters in recent weeks in an apparently coordinated cyber attack targeting research and academic institutions.

  Although officials sought to play down the seriousness of the threats, some security experts warned that such a break-in could potentially enable a serious attack on the internet.

  Stanford University, the San Diego Supercomputer Centre and the University of Illinois' National Centre for Supercomputing Applications (NSCA) were among the systems hit.

  http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/56002619?-2622
  Anick Jesdanun

- **ISS Makes Witty Patch Available to All**
  Internet Security Systems (ISS) has made a patch that protects two of its products (RealSecure and BlackIce) from the Witty worm available to everyone who owns the products. Last week, the company was criticized for making the patch available only to those customers whose maintenance contracts were current. The patch will be available for everyone through May 15, 2004.
  http://www.zdnet.co.uk/print/?TYPE=story&AT=39150909-39020375t-10000025c

- **Hackers Find Holes In WiFi Hot Spots Easy Entry Points**
  Digital intruders are piercing defenseless air space at corporations, public Wi-Fi hot spots and homes to gain illegal entry to computers. Gartner Group says about 90% of mobile devices lack protection.

http://www.usatoday.com/money/industries/technology/2004-04-13-hackers-wireless_x.htm

New Vulnerabilities Tested in SecureScout

- **19027 Adware AdBars**

  Adware: Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely displayed within the form of an ad-sponsored application.

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

  CVE Link: No CVE Match

  Reference: http://www.pestpatrol.com/PestInfo/a/adbars.asp

  19028 Adware AdBlaster

  Adware: Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely displayed within the form of an ad-sponsored application.

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

  CVE Link: No CVE Match

  Reference: http://www.pestpatrol.com/PestInfo/a/adblaster.asp

- **19029 Adware AdDestroyer**

  Adware: Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely displayed within the form of an ad-sponsored application.

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

  CVE Link: No CVE Match

  Reference: http://www.pestpatrol.com/PestInfo/a/addestroyer.asp

- **19030 Adware AdRoar**

  May display this message "This module was compiled with a trial version of Delphi. The trial period has expired.".

  Adware: Software that brings ads to your computer.
  Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely

displayed within the form of an ad-sponsored application.

Browser Helper Object: (BHO). A component that Internet Explorer will load whenever it starts, shares IE's memory context, can perform any action on the available windows and modules. A BHO can detect events, create windows to display additional information on a viewed page, monitor messages and actions. Microsoft calls it "a spy we send to infiltrate the browser's land." BHOs are not stopped by personal firewalls, because they are seen by the firewall as your browser itself. Some exploits of this technology search all pages you view in IE and replace banner advertisements with other ads. Some monitor and report on your actions. Some change your home page.

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

CVE Link: No CVE Match

Reference: http://www.pestpatrol.com/PestInfo/a/adroar.asp

- **19031 Adware AdRotator**

Adware: Software that brings ads to your computer.
Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely displayed within the form of an ad-sponsored application.

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

CVE Link: No CVE Match

Reference: http://www.pestpatrol.com/PestInfo/a/adrotator.asp

- **19032 Adware AdShooter/Searchforit**

Adware: Software that brings ads to your computer.
Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely displayed within the form of an ad-sponsored application.

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

CVE Link: No CVE Match

Reference: http://www.pestpatrol.com/PestInfo/a/adshooter_searchforit.asp

- **19033 Adware AdsStore**

Adware: Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely displayed within the form of an ad-sponsored application.

Toolbar: A group of buttons which perform common tasks. A toolbar for Internet Explorer is nomally located below the menu bar at the top of the form. Toolbars may be created by Browser Helper Objects.

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

CVE Link: No CVE Match

Reference: http://www.pestpatrol.com/PestInfo/a/adsstore.asp

- **19034 Adware Adult Material**

  Adware: Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely displayed within the form of an ad-sponsored application.

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

  CVE Link: No CVE Match

  Reference: http://www.pestpatrol.com/PestInfo/a/adult_material.asp

- **19035 Exploit ClickTillUWin (Dlder / Trojan.Win32.Dlder.a)**

  Exploit: A way of misusing or breaking into a system by taking advantage of a weakness in it.

  Alias: destructive program [F-Prot], Dlder [McAfee], Trojan.Win32.Dlder.a [Kaspersky]

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

  CVE Link: No CVE Match

  Reference: http://www.pestpatrol.com/PestInfo/c/clicktilluwin.asp

- **19036 Exploit HTASploit**

  Exploit: A way of misusing or breaking into a system by taking advantage of a weakness in it.

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

  CVE Link: No CVE Match

  Reference: http://www.pestpatrol.com/PestInfo/h/htasploit.asp

New Vulnerabilities found this Week

TA04-104A: Multiple Vulnerabilities in Microsoft Products

Security Bulletin MS04-011: Security Update for Microsoft Windows (835732)

This bulletin addresses 14 vulnerabilities affecting the systems listed below. There are several new vulnerabilities address by this bulletin, and several updates to previously reported vulnerabilities.

Remote attackers could execute arbitrary code on vulnerable systems.

Security Bulletin MS04-012: Cumulative Update for Microsoft RPC/DCOM (828741)

This bulletin addresses several new vulnerabilities affecting the systems listed below. These vulnerabilities are in Microsoft Windows Remote Procedure Call (RPC) and Distributed Component Object Model (DCOM).

Remote attackers could execute arbitrary code on vulnerable systems.

Security Bulletin MS04-013:Cumulative Security Update for Outlook Express (837009)

This bulletin addresses a vulnerability affecting the systems listed below. The vulnerability affects the Microsoft Windows MHTML Protocol handler and any applications that use it, including Microsoft Outlook and Internet Explorer. This vulnerability has been assigned VU#323070

and CAN-2004-0380.

Remote attackers could execute arbitrary code on vulnerable systems.

Microsoft has released a patch that addresses the cross-domain vulnerability discussed in TA04-099A: "Vulnerability in InternetExplorer ITS Protocol Handler". US-CERT is tracking this issue as VU#323070. This reference number corresponds to CVE candidate CAN-2004-0380.

Security Bulletin MS04-014: Vulnerability in the Microsoft Jet Database Engine Could Allow Code Execution (837001)

This bulletin addresses a vulnerability affecting the systems listed below. There is a buffer overflow vulnerability in Microsoft's Jet Database Engine (Jet). An attacker could take control of a vulnerable system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. This vulnerability has been assigned VU#740716 and CAN-2004-0197.

Remote attackers could execute arbitrary code on vulnerable systems.

For more information, see:

http://www.securityfocus.com/advisories/6558

https://www.microsoft.com/security/security_bulletins/200404_windows.asp

Mandrakelinux Security Update Advisory MDKSA-2004:030 tcpdump

A number of vulnerabilities were discovered in tcpdump versions prior to 3.8.1 that, if fed a maliciously crafted packet, could be exploited to crash tcpdump. These vulnerabilities include:

Remote attackers can cause a denial of service (crash) via ISAKMP packets containing a Delete payload with a large number of SPI's, which causes an out-of-bounds read. (CAN-2004-1083)

Integer underflow in the isakmp_id_print allows remote attackers to cause a denial of service (crash) via an ISAKMP packet with an Identification payload with a length that becomes less than 8 during byte order conversion, which causes an out-of-bounds read. (CAN-2004-0184)

For more information, see:

http://www.securityfocus.com/advisories/6558
http://www.securityfocus.com/advisories/6575
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0183
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0184

Debian Security Advisory DSA 485-1 ssmtp

Max Vozeler discovered two format string vulnerabilities in ssmtp, a simple mail transport agent. Untrusted values in the functions die() and log_event() were passed to printf-like functions as format strings. These vulnerabilities could potentially be exploited by a remote mail relay to gain the privileges of the ssmtp process (including potentially root).

For more information, see:

http://www.securityfocus.com/advisories/6572

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