netVigilance

ScoutNews Team **9 April 2004**
Issue #15

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

We are seeing security in WiFi driving recommendations and requirements for encryption that will drive new needs in Silicon and may even be a new beginning of a technology cycle – will be interesting to follow.
Microsoft donating to open source would be expected to support Microsoft's main business going forward.
Again we see an attempt to prove the ROI of IT activities – we all know it is there, but it is so difficult to agree on the measurement.
Enjoy the reading.

Top Security News Stories this Week

- **Defense Department WiFi Policy**
  The Defense Department's (DoD) soon to be released WiFi use policy will require that all data, both classified and unclassified, will have to be encrypted while traveling over wireless networks. The policy, DOD 8100.bb, is expected to be signed this week. In addition, DoD plans to create web sites with instructions for setting up wireless networks. DoD also plans to develop a cellular phone use policy.
  http://www.gcn.com/cgi-bin/udt/im.display.printable?client.id=gcndaily2&story.id=25462
  Joab Jackson

- **Air Force Network Security Exercise**
  About 200 people at Air Force network operation security centers and network control centers took part in a two-week computer network defense exercise. Dubbed Black Demon, the exercise involved managing network attacks, reconnaissance, denial-of-service, inside threats, malicious logic and loss of firewalls and network-defense tools.
  http://www.af.mil/news/story_print.asp?storyID=123007364
  Masao Doi

- **Microsoft Visits SourceForge.net / Microsoft Frees WiX**
  Late February, when Windows source code leaked to the Web even the most level-headed pundits could not foresee Microsoft's bits making their way to the Web in any other fashion. While some critics regard Microsoft as being notoriously proprietary and

dead set against the open source movement, the folks at Redmond have once again stunned the computing world and may have proven those critics wrong.

The latest contributor to SourceForge.net -- the largest open source developer network -- is none other than Microsoft itself. Microsoft's Windows Installer XML (WiX) has effectively been donated to the waiting hands of the open source community. As described by Microsoft, WiX is a toolset that builds Windows installation packages from XML code. The toolset is comprised of a compiler, a 'lib' tool, a 'linker' and a decompiler.
http://www.betanews.com/article.php3?sid=1081324871
David Worthington, BetaNews

- **Tracking the Blackout bug**

A number of factors and failings came together to make the August 14th northeastern blackout the worst outage in North American history. One of them was buried in a massive piece of software compiled from four million lines of C code and running on an energy management computer in Ohio.
To nobody's surprise, the final report on the blackout released by a US-Canadian task force Monday puts most of blame for the outage on Ohio-based FirstEnergy Corp., faulting poor communications, inadequate training, and the company's failure to trim back trees encroaching on high-voltage power lines. But over a dozen of task force's 46 recommendations for preventing future outages across North America are focused squarely on cyberspace.
http://www.theregister.co.uk/2004/04/08/blackout_bug_report/
Kevin Poulsen, Security Focus

- **Cisco warns of wireless security hole**

Networking equipment maker Cisco Systems Inc. is warning customers about a security hole in two products used to manage wireless LANs and e-business services in corporate data centers.
The company said on Wednesday that a user name and password coded into some versions of its Wireless LAN Solution Engine and Hosting Solution Engine software could give attackers complete control of the devices. Attackers could use the default logins to hide rogue wireless access points on wireless LANs, create and modify user privileges or change configuration settings, Cisco said. The vulnerability affects versions 2.0, 2.0.2 and 2.5 of the Wireless LAN Solution Engine (WLSE) and versions 1.7, 1.7.1, 1.7.2 and 1.7.3 of the Hosting Solution Engine (HSE). The San Jose, California, posted software patches on its Web site for both products.
http://www.infoworld.com/article/04/04/07/HNcisco_1.html
Paul Roberts, IDG News Service

- **Ballmer: Everyone has stake in cybersecurity**

Everyone, from computer users to software vendors to government agencies, is responsible for cybersecurity, Microsoft's chief executive officer (CEO) told a crowd in Washington, D.C., Wednesday.
Microsoft CEO Steve Ballmer did not outline new security initiatives in his speech at the Center for Strategic and International Studies, but he outlined the steps Microsoft has taken since its Chairman and Chief Software Architect Bill Gates called for security to become a top priority for the company in January 2002.
http://www.infoworld.com/article/04/04/07/HNcybersteve_1.html
Grant Gross, IDG News Service

- **Task force releases security recommendations**

  A computer industry task force that includes representatives from Microsoft Corp. and Computer Associates International Inc. issued its first round of recommendations on Thursday for improving software security, including a role for the U.S. government in supporting creation of secure software products.
  The U.S. Department of Homeland Security (DHS) should establish measurable annual security goals for the U.S. cybersecurity infrastructure and consider "tailored government action" to increase security in software development, according to a 123-page report from the National Cyber Security Partnership Task Force.
  http://www.infoworld.com/article/04/04/01/HNsecuretask_1.html
  Paul Roberts, IDG News Service

- **ROI: A Measure Of IT Success**

  If beauty is in the eye of the beholder, then IT success may well be in the eye of the CTO. Benefits arising from information technology continue to generate interest and debate among IT managers and CTOs. So how should an organization measure its IT success? For some companies, it might be as simple as just keeping the boss happy. This may not be the most effective approach, however. Dave Wreski, founder and CEO of Guardian Digital, says, “I don’t think it’s ever sufficient for IT to succeed only so far as to make the boss happy. Information technology should be an enabler, and if excessive resources are expended making sure the technology is operating the way it should or even through ongoing administration, then alternate solutions should be considered.”

  Using IT metrics, organizations can monitor the accomplishments of their IT goals and objectives. Success is determined by quantifying the level of implementation of security controls and the effectiveness and efficiency of those controls and by analyzing the adequacy of security activities and identifying possible improvements.
  http://www.processor.com/proeditorial/article.asp?article=articles%2Fp2615%2F31p15%2F31p15%2Easp&searchtype=&WordList=

New Vulnerabilities Tested in SecureScout

- **14251 SQL Server Remote Data Source Function Buffer Overflows Vulnerability**

  SQL Server is Microsoft SQL database for Windows platforms.
  This database is able to connect to remote data sources via "ad hoc" connections for connections that are seldom used. This is achieved through OLE DB providers.
  SQL Server is vulnerable to buffer overflows in OPENDATASOURCE and OPENROWSET. The syntax is something like SELECT * FROM OPENROWSET(buffer, '', ''). The buffer overflow occurs when the buffer size reaches about 7K bytes.
  The buffer overflows are known to be exploitable by untrusted users.

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

CVE Link: CAN-2002-0056

Initial advisory: http://marc.theaimsgroup.com/?l=vuln-ev&m=101413924631329&w=2
Microsoft Security Bulletin MS02-007:
http://www.microsoft.com/technet/security/bulletin/MS02-007.mspx
See also: http://www.securityfocus.com/bid/4135
Product page: http://www.microsoft.com/sql/default.asp

- **14382 W32/Netsky.p WormVulnerabilities in Microsoft Word and Microsoft Excel Could Allow Arbitrary Code to run (MS03-050/831527)**

A security vulnerability exists in Microsoft Excel that could allow malicious code execution. This vulnerability exists because of the method Excel uses to check the spreadsheet before reading the macro instructions. If successfully exploited, an attacker could craft a malicious file that could bypass the macro security model. If an affected spreadsheet was opened, this vulnerability could allow a malicious macro embedded in the file to be executed automatically, regardless of the level at which the macro security is set. The malicious macro could then take the same actions that the user had permissions to carry out, such as adding, changing or deleting data or files, communicating with a web site or formatting the hard drive.

A security vulnerability exists in Microsoft Word that could allow malicious code execution. This vulnerability exists due to to the way Word checks the length of a data value (Macro names) embedded in a document. If a specially crafted document were to be opened it could overflow a data value in Word and allow arbitrary code to be executed. If successfully exploited, an attacker could then take the same actions as the user had permissions to carry out, such as adding, changing or deleting data or files, communicating with a web site or formatting the hard drive.

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

CVE Link: CAN-2003-0820 & CAN-2003-0821

References:
http://www.microsoft.com/technet/security/bulletin/ms03-050.mspx

- **14421 Vulnerability in Microsoft Outlook Could Allow Code Execution (MS04-009/828040)**

A security vulnerability exists within Outlook 2002 that could allow Internet Explorer to execute script code in the Local Machine zone on an affected system. The parsing of specially crafted mailto URLs by Outlook 2002 causes this vulnerability. To exploit this vulnerability, an attacker would have to host a malicious Web site that contained a Web page designed to exploit the vulnerability and then persuade a user to view the Web page.

The attacker could also create an HTML e-mail message designed to exploit the vulnerability and persuade the user to view the HTML e-mail message. After the user has visited the malicious Web site or viewed the malicious HTML e-mail message an attacker who successfully exploited this vulnerability could access files on a user's

system or run arbitrary code on a user's system. This code would run in the security context of the currently logged-on user. Outlook 2002 is available as a separate product and is also included as part of Office XP.

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

CVE Link: CAN-2004-0121

References: http://www.microsoft.com/technet/security/Bulletin/MS04-009.mspx

- **14422 W32/Bagle.u Worm (Registry Check)**

This is a mass-mailing worm with the following characteristics:
* Contains its own SMTP engine to construct outgoing messages.
* Harvests email addresses from the victim machine
* The From: address of messages is spoofed
* Contains a remote access component (The worm sends notification via HTTP to a remote script (notification contains port number and ID number).
** Messages are constructed as follows **
From: (spoofed - using one of the harvested email addresses)
Subject: (blank)
Body: (blank)
Attachment: randomly named executable, with a .EXE extension
The worm installs itself into %SysDir% as GIGABIT.EXE, for example: C:\WINNT\SYSTEM32\GIGABIT.EXE
The worm checks the system date when it is executed - if it is the 1st January 2005 or later, it terminates.
** Method of Infection
** Mail Propagation
This virus constructs messages using its own SMTP engine. Target email addresses are harvested from files on the victim machine.
** Remote Access Component
The worm also opens a port on the victim machine - TCP port 4751.
The worm sends notification via HTTP to a remote script (notification contains port number and ID number). Users should block outgoing HTTP traffic to the following domain:
http://www.werde.de
The exact functionality offered by this backdoor is under investigation. It is suspected that it may allow for the downloading and execution of other files (akin to that for W32/Mydoom.a@MM).

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

CVE Link: No Mach to a CVE Link

References:http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101141

- **14423 W32/Netsky.q Worm (Registry Check)**

This virus spreads via email. It sends itself to addresses found on the victim's machine. (See SecureScout description for more detail)

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

CVE Link: No CVE link available
Reference: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101145

- **19022 Hijack EUniverse**

Adware supplied by eUniverse.com. KeenValue/v1 runs at startup, generates popup ads, and is the original version. KeenValue/Incredifind adds capability, via a second process:
monitors web sites visited, so that ads may be targeted;
hijacks the hosts file and redirects Netscape searches to incredifind.com;
hijacks error pages and address bar searches to incredifind.com, which is then redirected to sirsearch.com;
adds an Internet Explorer toolbar providing a search field directed to sirsearch.com.
'PerfectNav is designed to redirect your URL typing errors to PerfectNav's web page. This software helps keep Kazaa Media Desktop free.' --
http://www.kazaa.com/us/terms.htm

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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.

Downloader: A program designed to retrieve and install additional files, when run. Most will be configured to retrieve from a designated web or FTP site.

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

CVE Link: No CVE link available
Reference: http://www.pestpatrol.com/PestInfo/e/euniverse.asp

- **19023 Hijack Expext/MetaDirect**

Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

CVE Link: No CVE link available

Reference: http://www.pestpatrol.com/PestInfo/e/expext_metadirect.asp

- **19024 Hijack Find4u**

  Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

  CVE Link: No CVE link available

  Reference: http://www.pestpatrol.com/PestInfo/f/find4u.asp

- **19025 Hijack FreeScratchCards**

  Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

  CVE Link: No CVE link available

  Reference: http://www.pestpatrol.com/PestInfo/f/freescratchcards.asp

- **19026 Hijack Frsk**

  Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

  CVE Link: No CVE link available

  Reference: http://www.pestpatrol.com/PestInfo/f/frsk.asp

New Vulnerabilities found this Week

Internet Explorer and Outlook Express Status Bar Spoofing

« Execute arbitrary code with the privileges of the user running the browser »

This Internet Explorer (IE) vulnerability allows an attacker to trick a victim into visiting a malicious website. The attack occurs when a user clicks on a specially crafted hyperlink that, according to IE's status bar, points to a trusted site. Upon clicking the link, the browser is directed to a site of the attacker's choosing. The issue arises because IE does not properly display the destination URL when an
HTTP "FORM" element is embedded within the tags that define the hyperlink. To exploit the flaw, an attacker must entice a victim to follow a link provided in an HTML email or other HTML document (e.g. posted to a website). This vulnerability could potentially be exploited in concert with other unpatched IE flaws to execute arbitrary code with the privileges of the user running the browser. A proof-of-concept exploit has been publicly posted.

For more information, see:
http://archives.neohapsis.com/archives/ntbugtraq/2004-q1/0118.html
http://archives.neohapsis.com/archives/ntbugtraq/2004-q1/0121.html
http://www.malware.com/not-so-good.zip
http://www.securityfocus.com/bid/10023

HAHTsite Scenario Server Buffer Overflow
« Execute arbitrary code with "SYSTEM" privileges »

HAHTsite Scenario, an e-business server, is vulnerable to a stack-based buffer overflow. The flaw can be triggered by passing an overlong "projectname" to the "hsrun.exe" script, and exploited to execute arbitrary code with "SYSTEM" privileges (on Windows platforms). The technical details required to exploit the flaw have been posted. The discoverer of the flaw has also developed a proof-of-concept exploit that has not been publicly posted.

For more information, see:
http://www.protego.dk/advisories/20045.html
http://www.haht.com/
http://www.securityfocus.com/bid/10033

Macromedia Dreamweaver Database Connection Scripts
« Remote unauthenticated attacker can use the scripts to compromise the back-end database server »

The Macromedia Dreamweaver suite is designed for building web sites and web-related applications. The suite contains scripts that can be used for testing database connectivity in website configurations involving a back-end database. If these test scripts are not removed from the production website, a remote unauthenticated attacker can potentially use the scripts to compromise the back-end database server. The technical details required to exploit the flaw have been posted.

For more information, see:
http://archives.neohapsis.com/archives/vulnwatch/2004-q1/0075.html
http://www.macromedia.com/devnet/security/security_zone/mpsb04-05.html
http://secunia.com/advisories/11284

Gentoo Linux : Multiple Vulnerabilities in pwlib
« An attacker may cause a denial of service condition or cause a buffer overflow that would allow arbitrary code to be executed with root privileges »

pwlib is a multi-platform library designed for OpenH323. Multiple vulnerabilities have been found in the implementation of protocol H.323 contained in pwlib. Most of the vulnerabilities are in the parsing of ASN.1 elements which would allow an attacker to use a maliciously crafted ASN.1 element to cause unpredictable behavior in pwlib. An attacker may cause a denial of service condition or cause a buffer overflow that would allow arbitrary code to be executed with root privileges.

CVE: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0097
For more information, see:
http://www.uniras.gov.uk/vuls/2004/006489/h323.htm
http://www.securityfocus.com/advisories/6549

Gentoo Linux : iproute local Denial of Service vulnerability
« Local users could cause a Denial of Service »

iproute is a set of tools for managing linux network routing and advanced features.
It has been reported that iproute can accept spoofed messages on the kernel netlink interface from local users. This could lead to a local Denial of Service condition. Local users could cause a Denial of Service.

CVE: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0856
For more information, see: http://www.securityfocus.com/advisories/6548

OpenPKG : fetchmail
« Allows an attacker to cause a denial of service by sending a specially crafted email and crashing fetchmail »

According to a Mandrake Linux security advisory, a denial of service (DoS) vulnerability exists in the header rewriting code of Fetchmail. The code's intention is to hack message headers so replies work properly. However, logic in the reply_hack() function fails to allocate enough memory for long lines and may write past a memory boundary. This could allow an attacker to cause a denial of service by sending a specially crafted email and crashing fetchmail. The Common Vulnerabilities and exposures (CVE) project assigned the id CAN-2003-0792 to the problem.

For more information, see:
http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:101
http://www.securityfocus.com/advisories/6546

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