netVigilance

ScoutNews Team

23 April 2004
Issue #17

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

The basic TCP flaw shocked us all; Symantec claims that malicious code to exploit the TPC vulnerability already exists – we are all holding our breath hoping that the updates take care of this issue before we experience major DoS attack on the core of the Internet.
Super worms are predicted to be right around the corner – yes at netVigilance we believe they are: So….you better get safe and stay safe by implementing ongoing Vulnerability Management processes; or you will soon be asked to do so by someone who is unhappy that it was not in place earlier.
The emotional battle about whether open source is suitable for security products or not continues.
Philanthropically Microsoft turns its efforts towards the battle against child pornography on the Internet – Thumps up for this.

Enjoy reading

Top Security News Stories this Week

- **Experts warn of TCP vulnerability**
  Internet security experts warned Tuesday of a serious security vulnerability in the Transmission Control Protocol (TCP) a critical communications protocol used on the majority of computer networks in the world, according to an advisory from the United Kingdom's National Infrastructure Security Co-Ordination Centre (NISCC).
  The hole exists in all implementations of TCP that comply with the Internet Engineering Task Force's TCP specification. By exploiting the holes, malicious hackers could cause TCP sessions to end prematurely, creating a "denial of service," or DOS attack. The TCP vulnerability could also disrupt communications between routers on the Internet by interrupting BGP (Border Gateway Protocol) sessions that use TCP, NISCC said.
  http://www.infoworld.com/article/04/04/20/HNtcpwarning_1.html?source=rss&url=http://www.infoworld.com/article/04/04/20/HNtcpwarning_1.html
  Paul Roberts

- **Super Worms On The Way?**
  The threat from malicious Internet worms is about to explode exponentially, a security expert said Thursday as he predicted release of an especially menacing "super worm" in the near

future.
"The next super worm is about to hit," said Scott Chasin, chief technology officer at message filtering firm MX Logic and creator of the well-known security discussion group Bugtraq.
http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/56797967?-2622
Gregg Keizer

- **Code exists to exploit TCP flaw**
  Symantec has confirmed that malicious code that can take advantage of the Transmission Control Protocol flaw reported this week exists but says that the risk of real problems is remote
  Malicious code has been unearthed that can exploit a widely reported flaw in a popular Net protocol and possibly disrupt data transmissions, but experts say the risk of real-world problems remains fairly low.
  http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/56803256?-2622
  Michael Kanellos

- **Linux: unfit for national security?**
  Days after an embedded-industry CEO stirred up a firestorm by charging that Linux poses a threat to U.S. security, two prominent computing-security experts said last week that some developers are already inappropriately using Linux in critical security applications where it isn't suitable.
  Purdue University professor Eugene Spafford and Cynthia Irvine of the Naval Postgraduate School warned that the highest-level, but little-understood, security concerns are sometimes ignored during the development of control systems for tanks, bombs, missiles and defense aircraft. Linux, Windows and Solaris operating systems should not be used in such applications, Spafford said.
  http://www.eetimes.com/sys/news/showArticle.jhtml?articleID=18901858
  Charles J. Murray

- **Witchfinder General targets NSA in Warez sweep?**
  Taking a break from clearing the US airwaves of profanity, the DoJ's Witchfinder General John Ashcroft today boasted of a piracy sweep that has netted 200 computers in ten countries worldwide in the past twenty four hours.
  With help from the MPAA and RIAA, Operation Fastlink is a joint venture between the FBI's Cyber Division and the DoJ's Computer Crimes and Intellectual Property Section. The sweep has made 120 searches in the UK, Europe, Scandinavia and Singapore.
  http://www.theregister.co.uk/2004/04/22/doj_piracy_sweep/
  Andrew Orlowski

- **Task force issues more cybersecurity goals**
  IT vendors should improve default security settings in their products, a committee of the National Cyber Security Partnership Task Force (NCSP) said in a set of recommendations it has released on technical standards.
  The NCSP's Technical Standards and Common Criteria committee released its cybersecurity recommendations Monday, with the group of academics, government officials, IT vendors and customers asking vendors to provide stronger "out-of-the-box" security configurations and to support at least one configuration profile that provides a baseline security level.
  http://www.infoworld.com/article/04/04/19/HNtaskforce_1.html?source=rss&url=http://www.infoworld.com/article/04/04/19/HNtaskforce_1.html
  Grant Gross

- **Microsoft joins the fight against Internet paedophilia**

MICROSOFT, INTERPOL and The International Centre for Missing and Exploited Children have joined forces to battle the Internet's child pornography problem, and have formed the Global Campaign Against Child Pornography.
Sheila Johnson, an important member of the ICMEC board, donated $500,000 to the cause and was seeking another donor. Microsoft and ICMEC have had a history of working together, so apparently Microsoft was "a logical partner".
http://www.theinquirer.net/?article=15481
Tamlin Magee

New Vulnerabilities Tested in SecureScout

- **14424 Security Update for Microsoft Windows (MS04-011/835732)**

Buffer overrun vulnerability exists in LSASS that could allow remote code execution on an affected system. An attacker who successfully exploited this vulnerability could take complete control of the affected system.

A denial of service vulnerability exists that could allow an attacker to send a specially crafted LDAP message to a Windows 2000 domain controller. An attacker could cause the service responsible for authenticating users in an Active Directory domain to stop responding.

Buffer overrun vulnerability exists in the Private Communications Transport (PCT) protocol, which is part of the Microsoft Secure Sockets Layer (SSL) library. Only systems that have SSL enabled, and in some cases Windows 2000 domain controllers, are vulnerable. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Buffer overrun vulnerability exists in the Windows logon process (Winlogon). It does not check the size of a value used during the logon process before inserting it into the allocated buffer. The resulting overrun could allow an attacker to remotely execute code on an affected system. Systems that are not members of a domain are not affected by this vulnerability. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Buffer overrun vulnerability exists in the rendering of Windows Metafile (WMF) and Enhanced Metafile (EMF) image formats that could allow remote code execution on an affected system. Any program that renders WMF or EMF images on the affected systems could be vulnerable to this attack. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Remote code execution vulnerability exists in the Help and Support Center because of the way that it handles HCP URL validation. An attacker could exploit the vulnerability by constructing a malicious HCP URL that could potentially allow remote code execution if a user visited a malicious Web site or viewed a malicious e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Privilege elevation vulnerability exists in the way that Utility Manager launches applications. A logged-on user could force Utility Manager to start an application with system privileges and take complete control of the system.

Privilege elevation vulnerability exists in the way that Windows XP allows tasks to be created. Under special conditions, a non-privileged user could create a task that could execute with system permissions and therefore take complete control of the system.

Privilege elevation vulnerability exists in a programming interface that is used to create entries in the Local Descriptor Table (LDT). These entries contain information about segments of memory. An attacker who is logged on locally, could create a malicious entry and thereby gain access to protected memory, could take complete control of the system.

Remote code execution vulnerability exists in the way the Microsoft H.323 protocol implementation handles malformed requests. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Privilege elevation vulnerability exists in the operating system component that handles the Virtual DOS Machine (VDM) subsystem. This vulnerability could allow a logged on user to take complete control of the system.

Buffer overrun vulnerability exists in the Negotiate Security Software Provider (SSP) interface that could allow remote code execution. This vulnerability exists because of the way the Negotiate SSP interface validates a value that is used during authentication protocol selection. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A denial of service vulnerability exists in the Microsoft Secure Sockets Layer (SSL) library. The vulnerability results from the way that the Microsoft SSL library handles malformed SSL messages. This vulnerability could cause the affected system to stop accepting SSL connections on Windows 2000 and Windows XP. On Windows Server 2003, the vulnerability could cause the affected system to automatically restart.

Remote code execution vulnerability exists in the Microsoft ASN.1 Library. The vulnerability is caused by a possible "double-free" condition in the Microsoft ASN.1 Library that could lead to memory corruption on an affected system. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, under the most likely attack scenario this issue is a denial of service vulnerability.

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

CVE Links: CAN-2003-0533; CAN-2003-0663; CAN-2003-0719; CAN-2003-0806; CAN-2003-0906; CAN-2003-0907; CAN-2003-0908; CAN-2003-0909; CAN-2003-0910; CAN-2004-0117; CAN-2004-0118; CAN-2004-0119; CAN-2004-0120; CAN-2004-0123

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

- **14425 Cumulative Update for Microsoft RPC/DCOM (MS04-012/828741)**

Remote code execution vulnerability exists that results from a race condition when the RPC Runtime Library processes specially crafted messages. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, in the most likely attack scenario, this issue is a denial of service vulnerability.

A denial of service vulnerability exists in the RPCSS service. If a specially crafted message is sent to the RPCSS service, the service may not reclaim discarded memory. This behavior could result in a denial of service.

A denial of service vulnerability exists in the CIS and in the RPC over HTTP Proxy components. When a forwarded request to a backend system passes through them, an attacker could reply to the request by using a specially crafted message that could cause the affected components to stop accepting later requests.

A information disclosure vulnerability exists in the way that object identities are created. This vulnerability could allow an attacker to enable applications to open network communication ports. Although this vulnerability does not directly enable an attacker to compromise a system, it could be used to enable network communication through unexpected communication ports.

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

CVE Links: CAN-2003-0813; CAN-2004-0116; CAN-2003-0807; CAN-2004-0124

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-012.mspx

- **14426 Cumulative Security Update for Outlook Express (MS04-013/837009)**

A remote code execution vulnerability exists in the processing of specially crafted MHTML URLs that could allow an attacker's HTML code to run in the Local Machine security zone in Internet Explorer. This could allow an attacker to take complete control of an affected system.

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

CVE Link: CAN-2004-0380

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-013.mspx

- **14427 Vulnerability in the Microsoft Jet Database Engine Could Allow Code Execution (MS04-014/837001)**

A buffer overrun vulnerability exists in the Microsoft Jet Database Engine (Jet) that could allow remote code execution on an affected system. An attacker could exploit the vulnerability by creating a specially crafted database query and sending it through an application that is using Jet on an affected system. An attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges.

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

CVE Link: CAN-2004-0197

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-014.mspx

- **19037 Exploit Skull Burrow**

A simple program that allows you to relay a connection. This is much like a proxy server except this only allows you to forward to one address. Why would you want to loose the proxy? Because it's usually something you have no control over. Your proxy server is still logging activity. Skull Burrow solves this problem.

** Alias **
Backdoor.Skubur.a, Backdoor.Skubur.h, Backdoor.Skubur.i, Backdoor.Skubur.j, Backdoor.Skubur.l
Category: Exploit: A way of misusing or breaking into a system by taking advantage of a weakness in it.

** Variants **
Skull Burrow 1.0
Skull Burrow 2.0
Skull Burrow 3.0b
Skull Burrow 3b
Skull Burrow 3b (l)

Test Case Impact: **Gather Info** Vulnerability Impact: **Slows down the browser** Risk: **Low**

CVE Link: No CVE Match

Reference: http://www.pestpatrol.com/PestInfo/s/skull_burrow.asp

- **19037 Adware Advertbar**

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/advertbar.asp

New Vulnerabilities found this Week

Vulnerability Issues in TCP
NISCC Vulnerability Advisory 236929
Technical Cyber Security Alert TA04-111A

“Denial of Service”
“Border Gateway Protocol (BGP)”
“DNS (Domain Name System)”

The vulnerability described affects implementations of the Transmission Control Protocol (TCP) that comply with the Internet Engineering Task Force’s (IETF’s) Requests For Comments (RFCs) for TCP, including RFC 793, the original specification, and RFC 1323, TCP Extensions for High Performance.

TCP is a core network protocol used in the majority of networked computer systems today. Many vendors include support for this protocol in their products and may be impacted to varying degrees. Furthermore any network service or application that relies on a TCP connection will also be impacted, the severity depending primarily on the duration of the TCP session.

The impact of this vulnerability varies by vendor and application, but in some deployment scenarios it is rated critical. Please see the vendor section below for further information. Alternatively contact your vendor for product specific information.

If exploited, the vulnerability could allow an attacker to create a Denial of Service condition against existing TCP connections, resulting in premature session termination. The resulting session termination will affect the application layer, the nature and severity of the effects being dependent on the application layer protocol. The primary dependency is on the duration of the TCP connection, with a further dependency on knowledge of the network (IP) addresses of the end points of the TCP connection.

The Border Gateway Protocol (BGP) is judged to be potentially most affected by this vulnerability.

BGP relies on a persistent TCP session between BGP peers. Resetting the connection can result in medium term unavailability due to the need to rebuild routing tables and route flapping. Route flapping may result in route dampening (suppression) if the route flaps occur frequently within a short time interval. The overall impact on BGP is likely to be moderate based on the likelihood of successful attack. If the TCP MD5 Signature Option and anti-spoofing measures are used then the impact will be low as these measures will successfully mitigate the vulnerability.

There is a potential impact on other application protocols such as DNS (Domain Name System) and SSL (Secure Sockets Layer) in the case of zone transfers and ecommerce transactions respectively, but the duration of the sessions is relatively short and the sessions can be restarted without medium term unavailability problems. In the case of SSL it may be difficult to guess the source IP address.

Data injection may be possible. However, this has not been demonstrated and appears to be problematic.

For more information, see:
http://www.theregister.co.uk/2004/04/21/tcp_vuln/
www.securityfocus.com/news/8499
http://www.uniras.gov.uk/vuls/2004/236929/index.htm
http://www.us-cert.gov/cas/techalerts/TA04-111A.html

Denial of service vulnerabilities in OpenSSL
NetBSD Security Advisory 2004-005
“denial of service”

There are two distinct denial of service vulnerabilities addressed by this advisory:

1. Null-pointer assignment during SSL handshake:
A carefully crafted SSL/TLS handshake against a server which uses the OpenSSL library may result in a crash. Depending on how the application uses the OpenSSL library, this may result in a denial of service.

2. Out-of-bounds read affects Kerberos ciphersuites
A second flaw in the SSL/TLS handshake could cause a server configured to use the Kerberos ciphersuites to crash if a carefully crafted sequence of packets is sent by an attacker.

For more information, see:
http ://securityfocus.com/advisories/6611
ftp ://ftp.NetBSD.org/pub/NetBSD/security/advisories/NetBSD-SA2004-005.txt.asc

OpenPKG-SA-2004.015 : ethereal
“Arbitrary code execution”

According to a vendor security advisory [0] based on hints from Stefan Esser and Jonathan Heussser, several vulnerabilities of various types exist in the Ethereal network protocol analyzer [1]. Namely, it may be possible to make Ethereal crash or run arbitrary code by injecting a purposefully malformed packet onto the wire, by convincing someone to read a malformed packet trace file, or by creating a malformed color filter file.

The zero-length presentation protocol selector vulnerability named in the Ethereal vendor advisory does not affect OpenPKG though, because such presentation protocol selectors are not implemented in any Ethereal versions released by OpenPKG.

For more information, see:
http://securityfocus.com/advisories/6607
http://www.ethereal.com/appnotes/enpa-sa-00013.html

PostNuke Security Advisory PNSA 2004-2
“SQL injection”

PostNuke is a weblog/Content Management System (CMS). It is far more secure and stable than competing products, and able to work in high-volume environments with ease. Vulnerable versions can be exploited through SQL injection from the Comments and Your_Account modules included in the core package.

For more information, see:
http://securityfocus.com/advisories/6606
http://secunia.com/advisories/11386/

Debian Security Advisory DSA 494-1 ident2
“Buffer overflow”

Jack <jack@rapturesecurity.org> discovered a buffer overflow in ident2, an implementation of the ident protocol (RFC1413), where a buffer in the child_service function was slightly too small to hold all of the data which could be written into it. This vulnerability could be exploited by a remote attacker to execute arbitrary code with the privileges of the ident2 daemon (by default, the "identd" user).

For more information, see:
http://securityfocus.com/advisories/6613
http://security.debian.org/pool/updates/main/i/ident2/ident2_1.03-3woody1.dsc

Cisco Security Advisory: Vulnerabilities in SNMP Message Processing
“Device reload”

Cisco Internetwork Operating System (IOS) Software releases trains 12.0S, 12.1E, 12.2, 12.2S, 12.3, 12.3B and 12.3T may contain a vulnerability in processing SNMP requests which, if exploited, could cause the device to reload.

The vulnerability is only present in certain IOS releases on Cisco routers and switches. This behavior was introduced via a code change and is resolved with CSCed68575.

This vulnerability can be remotely triggered. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS).

For more information, see:
http://securityfocus.com/advisories/6605
http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml

Cisco Security Advisory: TCP Vulnerabilities in Multiple IOS-Based Cisco Products
“Denial Of Service / Reset any established TCP connection”

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

For more information, see:
http://securityfocus.com/advisories/6604

http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml

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