netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 14

April 4, 2008

Table of Contents

Product Focus

Much anticipated "Negev" in public Beta.

Try the New Beta Perimeter system, our Web-interface for the Perimeter Service is now running dynamic pages based on "Ajax", giving a much improved response time and customer experience. Existing customers can log right into the new system from the usual login page, The Rest of you should contact sales for a free trial.

Messenger Service Vulnerability Scanner – The Messenger Service Vulnerability Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Microsoft Windows Messenger Service flaw (MS03-043).

CTO Jesper Jurcenoks of netVigilance is the keynote speaker at the ITEC Conference & Exhibition 2008 in Houston May 8, see
http://www.netvigilance.com/events

This Week in Review

CERT fro open source on its way. Chris Sanders on packet analysis. Research report on email and spam. Will you beleive it: Google on Mars in 2050!...

Enjoy reading & Stay safe.

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

❖ Security Pros Launch Open-Source CERT

Backed by Google, a group of respected computer security pros launch oCERT, an effort to be the go-to place for security incident response for open-source projects.

Worried about the state of security incident response among open-source software projects, a group of computer security professionals has launched an ambitious effort to manage the coordination of vulnerability warnings and patch release information between open-source vendors large and small.

The new organization, called oCERT (Open Source Computer Emergency Response Team), emerged from stealth mode at this year's CanSecWest security conference with a grand plan to be the go-to place for security incident response when an open-source software project is affected.

eweek

Full Story :
http://www.eweek.com/c/a/Security/Security-Pros-Launch-Open-Source-CERT/

❖ Interview with Chris Sanders, Author of "Practical Packet Analysis"

Chris Sanders is a Senior Support Engineer for KeeFORCE, a technology consulting firm. Chris writes and speaks on various topics including packet analysis, network security, Microsoft technologies, and general network administration.

What are, in your opinion, the best tools for packet analysis?

If I were to be asked what tool I couldn't live without then it would definitely be Wireshark. Analyzing things at "the packet level" is really where the meat of network analysis is, and to do that you have to have a proper packet sniffing application.

Help net security

Full Story :
http://www.net-security.org/article.php?id=1124

❖ State of Internet security: protecting business email

Webroot released its latest research report, “State of Internet Security: Protecting Business Email.” The report reveals the significant impact that rapidly growing email security threats, in size and volume, are having on businesses worldwide and underscores the need for a multi-layered approach to Internet security.

Along with the rapid growth in spam, there is a similarly rapid growth in malware. Industry research shows that malware jumped from about 50,000 variants in 2004 to 5.5 million in 2007. Webroot research found that spam has become a significant vector of attack for

deploying these new malware variants.

Help net security

Full Story :
http://www.net-security.org/secworld.php?id=5961

- **Virgle: A Google/Virgin April Fool**

Google and Virgin have joined up to settle on Mars by the year 2050, Sophos can now recognize hackers based on their webcam videos and Gmail has managed to create an e-flux capacitor to send e-mails to the past and future. April Fools!

April 1 in the technology industry is always fun. Who can forget Opera's 2005 press release about a "short- and medium-range interpersonal communication" technology "enabling users to communicate in real- time without the use of computers or mobile phones"? Or how about the time that giant video game community GameFAQs turned into Xbox-exclusive GameFAX?

Tom's hardware

Full Story :
http://www.tomshardware.co.uk/Virgle-Google-Virgin,news-27861.html

New Vulnerabilities Tested in SecureScout

- **16390 Cisco IOS User Datagram Protocol Delivery Issue For IPv4/IPv6 Dual-stack Routers (cisco-sa-20080326-IPv4IPv6)**

A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

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

Some References:

* CISCO: 20080326 Cisco IOS User Datagram Protocol Delivery Issue For IPv4/IPv6 Dual-stack Routers
http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml
* FRSIRT: ADV-2008-1006
http://www.frsirt.com/english/advisories/2008/1006/references

CVE Reference: CVE-2008-1153

❖ 16391 Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS (cisco-sa-20080326-dlsw)

Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

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

References:

* CISCO: 20080326 Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS
http://www.cisco.com/en/US/products/products_security_advisory09186a0080969866.shtml
* BID: 28465
http://www.securityfocus.com/bid/28465
* FRSIRT: ADV-2008-1006
http://www.frsirt.com/english/advisories/2008/1006/references

CVE Reference: CVE-2008-1152

❖ 16746 Oracle Application Server - Oracle Reports Developer component unspecified Vulnerability (jan-2006/REP02)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Reports Developer component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
* CERT-VN: VU#545804
http://www.kb.cert.org/vuls/id/545804
* BID: 16287
http://www.securityfocus.com/bid/16287
* FRSIRT: ADV-2006-0243
http://www.frsirt.com/english/advisories/2006/0243
* FRSIRT: ADV-2006-0323
http://www.frsirt.com/english/advisories/2006/0323
* SECTRACK: 1015499
http://securitytracker.com/id?1015499
* SECUNIA: 18493
http://secunia.com/advisories/18493

* SECUNIA: 18608
http://secunia.com/advisories/18608
* XF: oracle-january2006-update(24321)
http://xforce.iss.net/xforce/xfdb/24321

CVE Reference: CVE-2006-0288

❖ 16747 Oracle Application Server - Oracle Reports Developer component unspecified Vulnerability (jan-2006/REP03)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Reports Developer component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
* CERT-VN: VU#545804
http://www.kb.cert.org/vuls/id/545804
* BID: 16287
http://www.securityfocus.com/bid/16287
* FRSIRT: ADV-2006-0243
http://www.frsirt.com/english/advisories/2006/0243
* FRSIRT: ADV-2006-0323
http://www.frsirt.com/english/advisories/2006/0323
* SECTRACK: 1015499
http://securitytracker.com/id?1015499
* SECUNIA: 18493
http://secunia.com/advisories/18493
* SECUNIA: 18608
http://secunia.com/advisories/18608
* XF: oracle-january2006-update(24321)
http://xforce.iss.net/xforce/xfdb/24321

CVE Reference: CVE-2006-0274

❖ 16748 Oracle Application Server - Oracle Reports Developer component unspecified Vulnerability (jan-2006/REP04)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Reports Developer component.

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

References:

* BUGTRAQ: 20060117 Oracle Reports - Read parts of files via customize(fixed after

875 days)
http://www.securityfocus.com/archive/1/archive/1/422261/30/7430/threaded
* MISC:
http://www.red-database-security.com/advisory/oracle_reports_read_any_xml_file.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
* CERT-VN: VU#545804
http://www.kb.cert.org/vuls/id/545804
* BID: 16287
http://www.securityfocus.com/bid/16287
* FRSIRT: ADV-2006-0243
http://www.frsirt.com/english/advisories/2006/0243
* FRSIRT: ADV-2006-0323
http://www.frsirt.com/english/advisories/2006/0323
* SECTRACK: 1015499
http://securitytracker.com/id?1015499
* SECUNIA: 18493
http://secunia.com/advisories/18493
* SECUNIA: 18608
http://secunia.com/advisories/18608
* XF: oracle-january2006-update(24321)
http://xforce.iss.net/xforce/xfdb/24321

CVE Reference: CVE-2006-0275

❖ 16749 Oracle Application Server - Oracle Reports Developer component unspecified Vulnerability (jan-2006/REP05)

An unspecified vulnerability with unknown impact exists in Oracle Application Server Oracle Reports Developer component.

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

References:

* BUGTRAQ: 20060117 Oracle Reports - Overwrite any application server file via desname (fixed after 889 days)
http://www.securityfocus.com/archive/1/archive/1/422257/30/7430/threaded
* BUGTRAQ: 20060117 Oracle Reports - Read parts of files via desname (fixed after 874 days)
http://www.securityfocus.com/archive/1/archive/1/422256/30/7430/threaded
* MISC:
http://www.red-database-security.com/advisory/oracle_reports_overwrite_any_file.html
* MISC:
http://www.red-database-security.com/advisory/oracle_reports_read_any_file.html
* CONFIRM:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html
* CERT-VN: VU#545804
http://www.kb.cert.org/vuls/id/545804
* BID: 16287

http://www.securityfocus.com/bid/16287
* FRSIRT: ADV-2006-0243
http://www.frsirt.com/english/advisories/2006/0243
* FRSIRT: ADV-2006-0323
http://www.frsirt.com/english/advisories/2006/0323
* SECTRACK: 1015499
http://securitytracker.com/id?1015499
* SECUNIA: 18493
http://secunia.com/advisories/18493
* SECUNIA: 18608
http://secunia.com/advisories/18608
* XF: oracle-january2006-update(24321)
http://xforce.iss.net/xforce/xfdb/24321

CVE Reference: CVE-2006-0289

❖ 16899 Cisco IOS Multicast Virtual Private Network (MVPN) Data Leak (cisco-sa-20080326-mvpn)

A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

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

References:

* CISCO: 20080326 Cisco IOS Multicast Virtual Private Network (MVPN) Data Leak
http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml
* FRSIRT: ADV-2008-1006
http://www.frsirt.com/english/advisories/2008/1006/references

CVE Reference: CVE-2008-1156

❖ 16900 Vulnerability in Cisco IOS with OSPF, MPLS VPN, and Supervisor 32, Supervisor 720, or Route Switch Processor 720 (cisco-sa-20080326-queue)

Certain Cisco Catalyst 6500 Series and Cisco 7600 Router devices that run branches of Cisco IOS based on 12.2 can be vulnerable to a denial of service vulnerability that can prevent any traffic from entering an affected interface. For a device to be vulnerable, it must be configured for Open Shortest Path First (OSPF) Sham-Link and Multi Protocol Label Switching (MPLS) Virtual Private Networking (VPN). This vulnerability only affects Cisco Catalyst 6500 Series or Catalyst 7600 Series devices with the Supervisor Engine 32 (Sup32), Supervisor Engine 720 (Sup720) or Route Switch Processor 720 (RSP720) modules. The Supervisor 32, Supervisor 720, Supervisor 720-3B, Supervisor 720-3BXL, Route Switch Processor 720, Route Switch Processor 720-3C, and Route Switch Processor 720-3CXL are all potentially vulnerable.

OSPF and MPLS VPNs are not enabled by default.

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

References:

* CISCO: 20080326 Vulnerability in Cisco IOS with OSPF, MPLS VPN, and Supervisor 32, Supervisor 720, or Route Switch Processor 720
http://www.cisco.com/warp/public/707/cisco-sa-20080326-queue.shtml
* FRSIRT: ADV-2008-1005
http://www.frsirt.com/english/advisories/2008/1005/references

CVE Reference: CVE-2008-0537

❖ 16901 Cisco IOS Virtual Private Dial-up Network Denial of Service Vulnerability (cisco-sa-20080326-pptp) (CSCsj58566)

Upon completion of a PPTP session, memory is leaked from the processor memory on the terminating device. This is shown in the output of show process memory under the *Dead* process. The *Dead* process is not a real process. Its function is to account for the memory that is allocated under the context of another process which has terminated, in this case PPTP. When the administrator is logged into the device, if the device is under exploitation, the Holding entry of the *Dead* process under the show process memory command will be increasing.

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

References:

* CISCO: 20080326 Cisco IOS Virtual Private Dial-up Network Denial of Service Vulnerability
http://www.cisco.com/en/US/products/products_security_advisory09186a008096
9862.shtml
* BID: 28460
http://www.securityfocus.com/bid/28460
* FRSIRT: ADV-2008-1006
http://www.frsirt.com/english/advisories/2008/1006/references
* SECTRACK: 1019714
http://securitytracker.com/id?1019714

CVE Reference: CVE-2008-1151

❖ 16902 Cisco IOS Virtual Private Dial-up Network Denial of Service Vulnerability (cisco-sa-20080326-pptp) (CSCdv59309)

Upon completion of a PPTP session, affected devices do not remove the virtual access interface that is associated with the PPTP session and do not reuse the interfaces in any future connections.

This situation can result in an exhaustion of the interface descriptor block (IDB) limit, which will prevent any new interfaces being created within Cisco IOS, effectively blocking all new VPDN connections, even though the router may still have enough processor memory to remain up and running. A reload of the device is required to

remove the interfaces.

An IDB is a Cisco IOS internal data structure that contains information such as the IP address, interface state, and packet statistics. Cisco IOS software maintains one IDB for each interface present on a platform and one IDB for each subinterface.

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

References:

* CISCO: 20080326 Cisco IOS Virtual Private Dial-up Network Denial of Service Vulnerability
http://www.cisco.com/en/US/products/products_security_advisory09186a008096 9862.shtml
* BID: 28460
http://www.securityfocus.com/bid/28460
* FRSIRT: ADV-2008-1006
http://www.frsirt.com/english/advisories/2008/1006/references
* SECTRACK: 1019714
http://securitytracker.com/id?1019714

CVE Reference: CVE-2008-1150

New Vulnerabilities found this Week

lighttpd OpenSSL Error Queue Denial of Service Vulnerability

"Denial of Service"

A vulnerability has been reported in lighttpd, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to lighttpd not properly clearing the OpenSSL error queue. This can be exploited to close concurrent SSL connections of lighttpd by terminating one SSL connection.

The vulnerability is reported in version 1.4.19. Other versions may also be affected.

References:
http://trac.lighttpd.net/trac/ticket/285

Sympa Malformed "Content-Type" Header Denial of Service Vulnerability

"Denial of Service"

A vulnerability has been reported in Sympa, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to a function call on an undefined value when processing mails with a specially crafted "Content-Type" header. This can be exploited to crash the service by sending a specially crafted email to a vulnerable system.

The vulnerability is reported in versions prior to 5.4.

References:
http://www.sympa.org/distribution/latest-stable/NEWS

GnuPG Duplicated IDs Memory Corruption

"Execution of arbitrary code"

A vulnerability has been reported in GnuPG, which can potentially be exploited to compromise a vulnerable system.

The vulnerability is caused due to an error when importing keys with duplicated IDs. This can be exploited to cause a memory corruption when importing keys via --refresh-keys or --import.

Successful exploitation potentially allows execution of arbitrary code, but has not been proven yet.

The vulnerability is reported in version 1.4.8 and 2.0.8. Prior versions may also be affected.

References:
http://lists.gnupg.org/pipermail/gnupg-announce/2008q1/000272.html

phpMyAdmin Username/Password Session File Information Disclosure

"Disclose sensitive information"

Jim Hermann has discovered a vulnerability in phpMyAdmin, which can potentially be exploited by malicious users to disclose sensitive information.

The MySQL username, password, and the Blowfish secret key are stored as plain text in session files. This can potentially be exploited e.g. by users on shared hosts to access that information.

The vulnerability is confirmed in version 2.11.5 and reported in all previous versions.

References:
http://www.phpmyadmin.net/home_page/security.php?issue=PMASA-2008-2

avast! Home/Professional aavmker4.sys Privilege Escalation

"Gain escalated privileges"

Tobias Klein has reported a vulnerability in avast! Home/Professional, which can be exploited by malicious, local users to gain escalated privileges.

An input validation error within the 0xb2d60030 IOCTL handler of the aavmker4.sys driver can be exploited e.g. to overwrite arbitrary kernel memory via a specially crafted IOCTL request.

The vulnerability is reported in version 4.7. Other versions may also be affected.

References:
http://www.avast.com/eng/avast-4-home_pro-revision-history.html

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