netVigilance

ScoutNews Team **3 September 2004**
Issue #36

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Due to the large amount of new information on vulnerabilities and test cases we have chosen to limit the number of news stories to only two this week.
Ballmer spoke of the great future of the software industry where security is seen to be the potential barrier, and then the story about large chunks of the computers in the Department of Defense and US Senate having been compromised and used as SPAM zombies.

Enjoy reading

Top Security News Stories this Week

❖ Ballmer Beats Security Drum

Microsoft CEO Steve Ballmer believes the software industry will create more positive change in the next 10 years than it did in the previous 10 -- provided that security threats are effectively handled.
"Security is the one issue that could stand in all our ways," Ballmer said in an address to the Massachusetts Software Council today. "To the degree that people don't feel they can rely on [applications] is a major impediment."

http://www.internetnews.com/bus-news/article.php/3402691
Colin Haley

❖ Hackers hijack federal computers

Hundreds of powerful computers at the Defense Department and U.S. Senate were hijacked by hackers who used them to send spam e-mail, federal authorities say.
The use of government computers was uncovered during the Justice Department (news - web sites)'s recent cybercrime crackdown. It adds another wrinkle to the use of so-called zombie PCs, which number in the millions and have bedeviled consumers and universities the past year.

http://story.news.yahoo.com/news?tmpl=story&cid=711&ncid=711&e=11&u=/usatoday/20040831/tc_usatoday/hackershijackfederalcomputers
Jon Swartz

New Vulnerabilities Tested in SecureScout

- **15491 Cisco IOS Malformed OSPF Packet Causes Reload (CSCec16481)**
  OSPF is a routing protocol defined by RFC 2328. It is designed to manage IP routing inside an Autonomous System (AS). OSPF packets use IP protocol number 89.

  A vulnerability exists in the processing of an OSPF packet that can be exploited to cause the reload of a system.

  Since OSPF needs to process unicast packets as well as multicast packets, this vulnerability can be exploited remotely. It is also possible for an attacker to target multiple systems on the local segment at a time.

  Using OSPF Authentication as described in the workarounds section can be used to mitigate the effects of this vulnerability. Using OSPF Authentication is a highly recommended security best practice

  A Cisco device receiving a malformed OSPF packet will reset and may take several minutes to become fully functional. This vulnerability may be exploited repeatedly resulting in an extended DOS attack. This issue is documented in bug ID CSCec16481.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml & http://www.securityfocus.com/bid/10971

- **15613 Vulnerabilities in H.323 Message Processing**
  H.323 is the International Telecommunications Union (ITU) standard for real-time multimedia communications and conferencing over packet-based (IP) networks. A subset of the H.323 standard is H.225.0, a standard used for call signalling protocols and media stream packetization over IP networks.

  The H.225.0 standard defines message formats for call setup, call control, and communications using Abstract Syntax Notation One (ASN.1). ITU Standard Q.931, which was developed for call signalling purposes in ISDN networks, is also used as the standard for the call setup messages within H.225.0.

  The vulnerabilities discovered in the affected products can be easily and repeatedly demonstrated with the use of the OUSPG PROTOS Test Suite for H.323. The largest group of vulnerabilities described in this advisory result from insufficient checking of H.225.0 messages as they are received and processed by an affected system. Malformed H.225.0 messages received by affected systems can cause various parsing and processing functions to fail, which may result in a system crash and reload (or reboot) in most circumstances.

  Typically, H.323 network elements implement call signalling over both UDP and TCP transports on port 1720. The H.323 test suite from OUSPG only tests the TCP implementation on port 1720 by default.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml & http://www.securityfocus.com/bid/9406

- **15755 Cisco IOS Software Processing of SAA Packets (CSCdx17916/CSCdx61997)**

  The RTR feature allows you to monitor network performance, network resources, and applications by measuring response times and availability. With this feature you can perform troubleshooting, problem notifications, and problem analysis based on response time reporter statistics.

  A router is vulnerable only if the RTR responder is enabled.

  By sending malformed RTR packets, it is possible to crash the router.

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

CVE Links: CAN-2003-0305

Reference: http://www.cisco.com/warp/public/707/cisco-sa-20030515-saa.shtml

- **15796 Cisco VPN 3000 Concentrator Vulnerabilities (CSCdea77143/CSCdz15393/CSCdt84906)**

  Enabling IPSec over TCP for a port on the VPN 3000 series concentrator allows TCP traffic on that port to traverse through the concentrator and reach the private network.

  For example, if one configures IPSec over TCP to use port 80 and the private network is routable to from the public network i.e. a workstation on the public network has the VPN 3000 series concentrator configured as the gateway for the private network IP address space, one can browse the web servers on the private network configured to serve port 80 from the workstation on the public network without any form of authentication. Another example, if IPSec over TCP was not configured for port 80 but was configured for its default port of 10000 and if there was a server listening for telnet connections on port 10000 on the private network, then one could telnet to that server from the workstation on the public network.

  A malformed SSH initialization packet sent during the initial SSH session setup may reload the VPN 3000 series concentrator.

  A flood of malformed ICMP packets could result in performance degradation on the VPN 3000 series concentrator and may even cause the concentrator to reload.

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

CVE Link: CAN-2003-0258 & CAN-2003-0259 & CAN-2003-0260

Reference: http://www.cisco.com/warp/public/707/cisco-sa-20030507-vpn3k.shtml

- **15806 Cisco Catalyst Enable Password Bypass Vulnerability (CSCea42030)**
  Anyone who can obtain command line access to an affected switch can bypass password authentication to obtain "enable" mode access without knowledge of the "enable" password. If local user authentication is enabled, any username can be used to gain access to the switch without a valid password. This same local user could then enter enable without a valid password.

  Command line access is provided through the console, telnet access, or ssh access methods; http access mode is not affected.

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

CVE Link: CAN-2003-0216

Reference: http://www.cisco.com/warp/public/707/cisco-sa-20030424-catos.shtml

- 17296 **Netscape Enterprise Web Server Authentication Vulnerability**
  Netscape Enterprise Server is a web server used to host larger-scale websites. A Web Publishing feature is installed by default. The Enterprise Server runs on Microsoft and most Unix and Linux platforms.
  An issue exists in Netscape Enterprise Server, which could allow an unauthorized user to brute force the password of user accounts when Web Publishing is enabled.
  Submitting a request containing 'wp-force-auth' will invoke an HTTP Basic Authentication dialog, from there users can use brute force techniques to potentially gain knowledge of the password, associated with known usernames (ie: guest, administrator, nobody etc.).
  It should be noted that iPlanet Web Server Enterprise Edition is also vulnerable to this issue.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.procheckup.com/security_info/vuln_pr0105.html & http://knowledgebase.iplanet.com/ikb/kb/articles/7764.html

- **17672 Bugzilla Cross-Site Scripting Vulnerabilities**
  Bugzilla is a free, open source bug tracking and reporting application. It allows users to submit bugs, offers a forum for discussing bugs, keeps track of the bug status, and can restrict who has access to bug information.
  An error exists in multiple versions of Bugzilla which may allow a remote attacker to carry out cross-site scripting attacks using default .html pages.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.securityfocus.com/bid/6868 & tp://www.bugzilla.org/

- **17636 Bugzilla SQL Injection Vulnerabilities**
  Bugzilla is a free, open source bug tracking and reporting application. It allows users to submit bugs, offers a forum for discussing bugs, keeps track of the bug status, and can restrict who has access to bug information.

  Multiple vulnerabilities including SQL Injection have been reported concerning BugZilla.

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

CVE Link: CAN-2003-0602 & CAN-2003-0603 & CAN-2003-1042 & CAN-2003-1043 & CAN-2003-1044 & CAN-2003-1045 & CAN-2003-1046

Reference: http://www.bugzilla.org/

- **17919 Mantis Input Validation Errors in 't_core_dir' PHP Code Injection Vulnerability**
  Mantis is a web-based bugtracking system. It is written in the PHP scripting language and requires the MySQL database and a webserver.

  It has been reported that if the REGISTER_GLOBAL variable is set, a remote user can specify the 't_core_dir' variable to cause PHP code at a remote site to be included and executed by the target system.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://securitytracker.com/alerts/2004/Aug/1011015.html

- **17920 SquirrelMail SquirrelSpell SQL Injection and XSS Vulnerabilities**
  Squirrelmail is a PHP based mail system designed for integration into an existing mail server system to allow a remote user to access his mail via the web.

  Input validation vulnerabilities have been reported in SquirrelMail. A remote user may be able to execute SQL statements or perform Cross-Site-Scripting (XSS) attacks.

  If SquirrelMail is configured to store user address books in the database, a remote attacker can exploit a flaw based on lookup function from 'abook_database.php' to execute arbitrary SQL statements.

  Multiple cross-site scripting (XSS) vulnerabilities have been reported via multiple attack vectors, including the mailbox parameter in compose.php.

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

CVE Link: CAN-2004-0521 & CAN-2004-0520 & CAN-2004-0519

Reference: http://www.squirrelmail.org & http://www.rs-labs.com/adv/RS-Labs-Advisory-2004-1.txt & http://marc.theaimsgroup.com/?l=squirrelmail-cvs&m=108309375029888

New Vulnerabilities found this Week

- **Cisco Security Advisory: Vulnerabilities in Kerberos 5 Implementation**
  “Remote code execution and Denial of Service”

  Two vulnerabilities in the Massachusetts Institute of Technology (MIT) Kerberos 5 implementation that affect Cisco VPN 3000 Series Concentrators have been announced by the MIT Kerberos Team.
  Cisco VPN 3000 Series Concentrators authenticating users against a Kerberos Key Distribution Center (KDC) may be vulnerable to remote code execution and to Denial of Service (DoS) attacks. Cisco has made free software available to address these problems. Cisco VPN 3000 Series Concentrators not authenticating users against a Kerberos Key Distribution Center (KDC) are not impacted.

  No exploitations of these vulnerabilities have been reported.
  An exploitation of the double-free vulnerability could potentially give an attacker control of the Cisco device and potentially compromise an entire Kerberos realm.
  An exploitation of the "infinite loop in the ASN.1 decoder" vulnerability could potentially take out of service an affected product. The vulnerability could potentially be repeatedly exploited to keep the product out of service until an upgrade can be performed.

  References: http://www.cisco.com/warp/public/707/cisco-sa-20040831-krb5.shtml.

- **Cisco Security Advisory: Cisco Telnet Denial of Service Vulnerability**
  “Deny remote access to the device”

  A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS)® may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Data Link Switching (DLSw) and protocol translation connections may also be affected. Telnet, reverse telnet, RSH, SSH, DLSw and protocol translation sessions established prior to exploitation are not affected.
  All other device services will operate normally. Services such as packet forwarding (excluding DLSw and protocol translation per above), routing protocols and all other communication to and through the device are not affected.

  Exploitation of this vulnerability may result in the denial of new telnet, reverse telnet, RSH, SSH, SCP, DLSw, protocol translation and HTTP connections to a device running IOS. Other access to the device via the console or SNMP is not affected. The device will remain in this state until the problematic TCP connection is cleared, or the device is reloaded (which will clear the problematic session). If no other access methods are available, exploitation of this vulnerability could deny remote access to the device.
  Depending on your network architecture, workarounds may be available to mitigate this vulnerability.

  References: http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml.

❖ Cisco Security Advisory: Multiple Vulnerabilities in Cisco Secure Access Control Server

"Multiple Denial of Service (DoS) and authentication related vulnerabilities"

Cisco Secure Access Control Server for Windows (ACS Windows) and Cisco Secure Access Control Server Solution Engine (ACS Solution Engine) provide authentication, authorization, and accounting (AAA) services to network devices such as a network access server, Cisco PIX and a router. This advisory documents multiple Denial of Service (DoS) and authentication related vulnerabilities for the ACS Windows and the ACS Solution Engine servers.

These vulnerabilities may:
* Cause a crash impacting the availability of services on the ACS devices. Until the device is rebooted a DoS is the result.
* May allow unauthorized users to access AAA clients without an effective password (using blank passwords) if the bind to the NDS database is anonymous.
* May allow unauthenticated users to gain access to the ACS Administration GUI.

References: http://www.cisco.com/warp/public/707/cisco-sa-20040825-acs.shtml.

❖ Cisco Security Advisory: Cisco IOS Malformed OSPF Packet Causes Reload

"Reload of the device"

A Cisco device running Internetwork Operating System (IOS) ® and enabled for the Open Shortest Path First (OSPF) protocol is vulnerable to a Denial of Service (DoS) attack from a malformed OSPF packet. The OSPF protocol is not enabled by default.
The vulnerability is only present in Cisco IOS release trains based on 12.0S, 12.2, and 12.3. Releases based on 12.0, 12.1 mainlines, and all Cisco IOS images prior to 12.0 are not affected.
There are workarounds available to mitigate the effects.

Successful exploitation of this vulnerability results in a reload of the device. Repeated exploitation could result in a sustained DoS attack.

References: http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml.

❖ DB2 Multiple Unspecified Vulnerabilities

"Execute arbitrary code"

NGSSoftware has reported multiple unspecified vulnerabilities in DB2 Universal Database, allowing malicious people to compromise a vulnerable system.

Two of the vulnerabilities are caused due to boundary errors, which can be exploited to execute arbitrary code. There are also some other unspecified errors with an unknown impact.

The vulnerabilities have been reported in the following versions:
* DB2 8.1 Fixpak 6 and prior

* DB2 7.x Fixpak 11 and prior

http://www.nextgenss.com/advisories/db2-01.txt

- **LHA Multiple Vulnerabilities**

"Execution of arbitrary code"
Multiple vulnerabilities have been reported in LHA, which can be exploited by malicious people to compromise a user's system.

1) A vulnerability caused due to boundary errors in the parsing of archives can be exploited using a specially crafted archive to cause a buffer overflow when a user extracts or tests the archive.

Successful exploitation may allow execution of arbitrary code.

2) Some boundary errors in the parsing of command-line arguments can be exploited using a specially crafted command-line argument to cause a buffer overflow.

Successful exploitation may allow execution of arbitrary code.

3) A vulnerability caused due to insufficient validation of shell meta characters in directories can be exploited to inject arbitrary shell commands.

The vulnerabilities have been reported in version 1.14 and prior.

References: http://rhn.redhat.com/errata/RHSA-2004-323.html

- **Winzip Unspecified Multiple Buffer Overflow Vulnerabilities**

"Execution of arbitrary code"

Multiple vulnerabilities has been reported in Winzip, which potentially can be exploited to compromise a user's system.

1) Some unspecified vulnerabilities which can be exploited to cause buffer overflows. Successful exploitation can potentially lead to execution of arbitrary code.

2) A problem caused due to insufficient validation of command-line arguments. This can be exploited by using a specially crafted argument to cause a buffer overflow and potentially execute arbitrary code.

References: http://secunia.com/advisories/12430/

- **WFTPD Pro Server MLST Command Denial of Service Vulnerability**

"Denial of Service"

lion has discovered a vulnerability in WFTPD Pro Server, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to insufficient validation of the MLST command. This can be exploited by sending over 60 MLST commands with overly long arguments. Successful exploitation causes the FTP server to crash.

The vulnerability has been confirmed on version 3.21.3.1. Other versions may also be affected.

References: http://seclists.org/lists/bugtraq/2004/Aug/0408.html

❖ WS_FTP Server File Path Parsing Denial of Service Vulnerability

“Denial of Service”

lion has discovered a vulnerability in WS_FTP Server, which can be exploited by malicious users to cause a DoS (Denial of Service).

The problem is caused due to an error in the parsing of file paths and can be exploited to cause a vulnerable system to use a large amount of CPU resources.

Successful exploitation requires that the user has been authenticated.

The vulnerability has been confirmed on version 5.0.2. Other versions may also be affected.

References: http://secunia.com/advisories/12406/

❖ Oracle Products Multiple Unspecified Vulnerabilities

“Denial of Service or SQL injection attacks”

Multiple vulnerabilities with an unknown impact have been reported in various Oracle products. Reportedly, some of the vulnerabilities can be exploited to compromise a vulnerable system, cause a DoS (Denial of Service), or conduct SQL injection attacks.

1) Various unspecified vulnerabilities exist in the Database Server and the Listener. The vendor rates the exposure risk as high and states that exploitation of some of the vulnerabilities requires network access, but no valid user account.

2) Various unspecified vulnerabilities exist in Oracle Application Server within the Portal and iSQL*Plus components. The vendor rates the exposure risk as high and states that exploitation of some of the vulnerabilities requires network access, but no valid user account.

3) Various unspecified vulnerabilities exist in Oracle Enterprise Manager. The vendor rates the exposure risk as medium and states that exploitation requires a valid user account on a vulnerable system.

The following products are affected:
* Oracle Database 10g Release 1, version 10.1.0.2
* Oracle9i Database Server Release 2, versions 9.2.0.4 and 9.2.0.5
* Oracle9i Database Server Release 1, versions 9.0.1.4, 9.0.1.5 and 9.0.4
* Oracle8i Database Server Release 3, version 8.1.7.4
* Oracle Enterprise Manager Grid Control 10g, version 10.1.0.2
* Oracle Enterprise Manager Database Control 10g, version 10.1.0.2

* Oracle Application Server 10g (9.0.4), versions 9.0.4.0 and 9.0.4.1
* Oracle9i Application Server Release 2, versions 9.0.2.3 and 9.0.3.1
* Oracle9i Application Server Release 1, version 1.0.2.2

References:
http://otn.oracle.com/deploy/security/pdf/2004alert68.pdf
http://www.kb.cert.org/vuls/id/435974
http://www.kb.cert.org/vuls/id/316206

❖ Kerberos V5 Multiple Vulnerabilities

Multiple vulnerabilities have been reported in Kerberos V5, where the most serious potentially can be exploited by malicious people to compromise a vulnerable system.

1) Various double-free errors within the KDC (Key Distribution Center) cleanup code and in client libraries may allow unauthenticated people to execute arbitrary code on an affected system. The problem is that the ASN.1 decoding functions may free an allocated buffer on the heap, which may then be freed again later by either the KDC cleanup functionality or certain library functions.

This vulnerability affects version 1.3.4 and prior.

2) Some double-free errors within the "krb5_rd_cred()" function may allow authenticated users to execute arbitrary code on an affected system. The problem is that the function attempts to free an allocated buffer on the heap, which has already been freed by the ASN.1 decoding function when an error is encountered.

This can be exploited via affected services calling the vulnerable function (e.g. krshd, klogind, and telnetd).

This vulnerability affects version 1.3.1 and prior.

3) A double-free error within krb524d may allow execution of arbitrary code. The problem is that a buffer allocated on the heap is freed, when conversion of a cross-realm ticket is denied and then later freed again when calling the "krb5_free_ticket()" function.

This vulnerability affects version 1.2.8 through 1.3.4.

4) An error within the ASN.1 decoder when handling indefinite length BER encodings can be exploited by unauthenticated people to cause a vulnerable system to hang in an infinite loop via a specially crafted BER encoding.

This vulnerability affects versions 1.2.2 through 1.3.4.

References:
http://web.mit.edu/kerberos/www/.../MITKRB5-SA-2004-002-dblfree.txt
http://web.mit.edu/kerberos/www/...ies/MITKRB5-SA-2004-003-asn1.txt
http://www.kb.cert.org/vuls/id/795632
http://www.kb.cert.org/vuls/id/866472

❖ OpenBSD ICMP Denial of Service Vulnerability

“Crash a vulnerable system”

Vafa Izadinia has reported a vulnerability in OpenBSD, which can be exploited by malicious people to conduct DoS (Denial of Service) attacks.

The problem is caused due to insufficient validation of ICMP packets and can be exploited to crash a vulnerable system via a specially crafted ICMP packet sent from one interface to another.

Successful exploitation requires that the system has been setup to act as a bridge between two networks and has IPsec processing enabled.

References:
* OpenBSD 3.5:
ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/016_bridge.patch
* OpenBSD 3.4:
ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.4/common/028_bridge.patch

❖ Apache 2 mod_ssl Connection Abort Denial of Service

“Denial of Service”
A vulnerability has been reported in Apache 2 mod_ssl, which can be exploited by malicious people to cause a DoS (Denial of Service).

The problem is that it is possible to cause mod_ssl to enter an infinite loop by aborting a SSL connection in a particular state. This causes the process to consume large amounts of CPU resources.

This has been reported in Apache 2.0.50 and prior.

References: http://rhn.redhat.com/errata/RHSA-2004-349.html

❖ Linux Kernel NFS and ptmx Denial of Service Vulnerabilities

“Denial of Service”
Two vulnerabilities have been reported in the Linux Kernel, allowing malicious people to cause a DoS (Denial of Service).

1) The problem is caused due to signedness errors which can lead to integer overflows in the XDR decode functions in kNFSd. This can be exploited by sending packets with a write request larger than 2^31, causing the system to crash.

2) An unspecified vulnerability in "/dev/ptmx" allows malicious local users to cause a DoS.

This has been reported in the Linux Kernel 2.6 branch.

References: http://www.suse.de/de/security/2004_28_kernel.html

❖ Citadel/UX Username Buffer Overflow Vulnerability

“Execute arbitrary code”

A buffer overrun vulnerability is reported for Citadel/UX. The problem occurs due to insufficient bounds checking when processing 'USER' command arguments.

An anonymous remote attacker may be capable of exploiting this issue to execute arbitrary code. This however has not been confirmed. Failed exploit attempts may result in a denial of service.

References: http://www.securityfocus.com/bid/10833/discussion/

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