netVigilance

ScoutNews Team **September 30, 2005**
Issue # 39

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Corporations have trouble assessing risk to their networks, yet identify network security as their chief concern??

Enjoy reading

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

Top Security News Stories this Week

- **Greater percentage of U.S. / U.K. business unable to determine if networks are secure**

CIOs and CSOs at over one-half of the 1800 polled; could not deliver a risk assessment audit if asked.

Despite this being the primary concern of CIOs for 2005 (see below), little progress seems to have been made. No data was offered as to why the most critical function of a modern IT department is somehow neglected.

An occasional perimeter test wouldn't hurt, people – *Ed.*

IT-Observer

Full Story :

http://www.ebcvg.com/articles.php?id=918

❖ Security [still] chief IT concern for enterprises

In a recent survey conducted by Nortel, enterprise business managers are still listing network security as their primary concern.

This parallels findings from a survey done by Robert Half Technology in February of this year.

IT-Observer

Full Story:
http://www.ebcvg.com/articles.php?id=912

❖ Checkpoint discloses serious firmware flaw

Checkpoint announced that several models of their firewall products contain a bug that can allow non-CIFS traffic to get passed through as CIFS traffic or completely deny all CIFS traffic.

At time of press, Checkpoint did not have a fix for this problem.

eWeek

Related Links:
http://www.eweek.com/article2/0,1895,1863233,00.asp

New Vulnerabilities Tested in SecureScout

❖ 15240 BIND Denial of service via maxdname Vulnerability

Improper handling of certain data copied from the network could allow a remote intruder to disrupt the normal operation of your name server, possibly including a crash.

The issue affects version 8.2 through 8.2.2-P2 and version 4.9 through 4.9.7-REL.

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

References:

Original Advisory:
http://www.isc.org/index.pl?/sw/bind/bind-security.php

Other References:
SUSE:19991111 Security hole in bind8 < 8.2.2p2 and bind4 < 4.9.7-REL
DEBIAN:19991116 Denial of service vulnerabilities in bind
CALDERA:CSSA-1999-034.1
REDHAT:RHSA-1999:054-01
SUN:00194
CERT:CA-99-14
BID:788
XF:bind-maxdname-bo

Product HomePage:
http://www.isc.org/index.pl?/sw/bind/

CVE Reference: CVE-1999-0849

❖ **15241 BIND Denial of service via consuming more than "fdmax" file descriptors Vulnerability**

Remote intruders can consume more file descriptors than BIND can properly manage, causing named to crash.

The issue affects version 8.2 through 8.2.2-P2 and version 4.9 through 4.9.7-REL.

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

References:

Original Advisory:
http://www.isc.org/index.pl?/sw/bind/bind-security.php

Other References:
SUSE:19991111 Security hole in bind8 < 8.2.2p2 and bind4 < 4.9.7-REL
DEBIAN:19991116 Denial of service vulnerabilities in bind
CALDERA:CSSA-1999-034.1
REDHAT:RHSA-1999:054-01
SUN:00194
CERT:CA-99-14
BID:788
XF:bind-fdmax-dos

Product HomePage:
http://www.isc.org/index.pl?/sw/bind/

CVE Reference: CVE-1999-0848

❖ **15242 BIND Denial of service by improperly closing TCP sessions via so_linger Vulnerability**

By intentionally violating the expected protocols for closing a TCP session, remote intruders can cause named to pause for periods up to 120 seconds.

The issue affects version 8.2 through 8.2.2-P2 and version 4.9 through 4.9.7-REL.

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

References:

Original Advisory:
http://www.isc.org/index.pl?/sw/bind/bind-security.php

Other References:
SUSE:19991111 Security hole in bind8 < 8.2.2p2 and bind4 < 4.9.7-REL
DEBIAN:19991116 Denial of service vulnerabilities in bind
CALDERA:CSSA-1999-034.1
REDHAT:RHSA-1999:054-01
SUN:00194
CERT:CA-99-14
XF:bind-solinger-dos
BID:788

Product HomePage:
http://www.isc.org/index.pl?/sw/bind/

CVE Reference: CVE-1999-0837

❖ **15243 BIND Denial of service via malformed SIG records Vulnerability**

This vulnerability involves a failure to properly validate SIG records, allowing a remote intruder to crash named; see the impact section for additional details.

The issue affects version 8.2 through 8.2.2-P2 and version 4.9 through 4.9.7-REL.

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

References:

Original Advisory:
http://www.isc.org/index.pl?/sw/bind/bind-security.php

Other References:
SUSE:19991111 Security hole in bind8 < 8.2.2p2 and bind4 < 4.9.7-REL
DEBIAN:19991116 Denial of service vulnerabilities in bind
CALDERA:CSSA-1999-034.1
REDHAT:RHSA-1999:054-01
CERT:CA-99-14
XF:bind-sigrecord-dos
BID:788

Product HomePage:
http://www.isc.org/index.pl?/sw/bind/

CVE Reference: CVE-1999-0835

❖ **15244 BIND Denial of service via naptr Vulnerability**

Some versions of BIND fail to validate zone information loaded from disk files. In

environments with unusual combinations of permissions and protections, this could allow an intruder to crash named.

The issue affects version 8.2 through 8.2.2-P2 and version 4.9 through 4.9.7-REL.

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

References:

Original Advisory:
http://www.isc.org/index.pl?/sw/bind/bind-security.php

Other References:
SUSE:19991111 Security hole in bind8 < 8.2.2p2 and bind4 < 4.9.7-REL
DEBIAN:19991116 Denial of service vulnerabilities in bind
CALDERA:CSSA-1999-034.1
REDHAT:RHSA-1999:054-01
SUN:00194
CERT:CA-99-14
BID:788
XF:bind-naptr-dos

Product HomePage:
http://www.isc.org/index.pl?/sw/bind/

CVE Reference: CVE-1999-0851

❖ **15245 BIND DNS cache poisoning by predictable query IDs Vulnerability**

The mapping between host names and IP addresses may be changed. As a result, attackers can inspect, capture, or corrupt the information exchanged between hosts on a network.

The issue affects version 4.9 through 4.9.6 no included.

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

References:

Original Advisory:
http://www.isc.org/index.pl?/sw/bind/bind-security.php

Other References:
CERT:CA-97.22.bind
XF:bind
NAI:NAI-11

Product HomePage:
http://www.isc.org/index.pl?/sw/bind/

CVE Reference: CVE-1999-0024

❖ 15246 BIND Denial of Service vulnerabilities via CNAME record and zone transfer

BIND 4.9 releases prior to BIND 4.9.7 and BIND 8 releases prior to 8.1.2 do not properly bounds check many memory references in the server and the resolver. An improperly or maliciously formatted DNS message can cause the server to read from invalid memory locations, yielding garbage record data or crashing the server. Many DNS utilities that process DNS messages (e.g., dig, nslookup) also fail to do proper bounds checking.

Any system running BIND 4.9 prior to 4.9.7 or BIND 8 prior to 8.1.2 is vulnerable.

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

References:

Original Advisory:
http://www.isc.org/index.pl?/sw/bind/bind-security.php

Other References:
CERT:CA-98.05.bind_problems
SGI:19980603-01-PX
HP:HPSBUX9808-083
SUN:00180
XF:bind-axfr-dos

Product HomePage:
http://www.isc.org/index.pl?/sw/bind/

CVE Reference: CVE-1999-0011

❖ 15247 BIND Denial of Service vulnerability via maliciously formatted DNS messages

Assume that the following self-referential resource record is in the cache on a name server:

foo.example. IN A CNAME foo.example.

The actual domain name used does not matter; the important thing is that the target of the CNAME is the same name. The record could be in the cache either because the server was authoritative for it or because the server is recursive and someone asked for it. Once this record is in the cache, issuing a zone transfer request using its name (e.g., "dig @my_nameserver foo.example. axfr") will cause the server to abort().

Most sites will not contain such a record in their configuration files. However, it is possible for an attacker to engineer such a record into the cache of a vulnerable nameserver and thus cause a denial of service.

Any system running BIND 8 prior to 8.1.2 is vulnerable.

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

References:

Original Advisory:
http://www.isc.org/index.pl?/sw/bind/bind-security.php

Other References:
CERT:CA-98.05.bind_problems
SGI:19980603-01-PX
HP:HPSBUX9808-083
XF:bind-dos

Product HomePage:
http://www.isc.org/index.pl?/sw/bind/

CVE Reference: CVE-1999-0010

❖ **15248 BIND Inverse query buffer overflow Vulnerability**

BIND 4.9 releases prior to BIND 4.9.7 and BIND 8 releases prior to 8.1.2 do not properly bounds check a memory copy when responding to an inverse query request. An improperly or maliciously formatted inverse query on a TCP stream can crash the server or allow an attacker to gain root privileges.

Any system running BIND 4.9 prior to 4.9.7 is vulnerable.
Any system running BIND 8 prior to 8.1.2 is vulnerable.

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

References:

Original Advisory:
http://www.isc.org/index.pl?/sw/bind/bind-security.php

Other References:
SGI:19980603-01-PX
HP:HPSBUX9808-083
SUN:00180
CERT:CA-98.05.bind_problems
XF:bind-bo
BID:134

Product HomePage:
http://www.isc.org/index.pl?/sw/bind/

CVE Reference: CVE-1999-0009

❖ **15689 Opera Download Dialog Spoofing Vulnerability (Remote File Checking)**

Secunia Research has discovered a vulnerability in Opera, which can be exploited by malicious people to trick users into executing malicious files.

The vulnerability is caused due to an error in the handling of extended ASCII codes in the download dialog. This can be exploited to spoof the file extension in the file download dialog via a specially crafted "Content-Disposition" HTTP header.

Successful exploitation may result in users being tricked into executing a malicious file via the download dialog, but requires that the "Arial Unicode MS" font (ARIALUNI.TTF) has been installed on the system.

NOTE: The "Arial Unicode MS" font is installed with various Microsoft Office distributions.

The vulnerability has been confirmed in version 8.01. Other versions may also be affected.

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

References:

Original Advisory:
http://secunia.com/advisories/15870/

Product HomePage:
http://www.opera.com/

CVE Reference: CAN-2005-2405

New Vulnerabilities found this Week

- **AIX "getconf" Command Buffer Overflow Vulnerability**
  "Gain escalated privileges"

  A vulnerability has been reported in AIX, which can be exploited by malicious, local users to gain escalated privileges.

  The vulnerability is caused due to an unspecified boundary error in the "getconf" command, which is part of the bos.rte.shell fileset. This can be exploited to cause a buffer overflow and allows arbitrary code execution with root privileges.

  The vulnerability has been reported in AIX 5.2.0 and 5.3.0.

  References:
  http://www-1.ibm.com/support/docview.wss?uid=isg1IY73850
  http://www-1.ibm.com/support/docview.wss?uid=isg1IY73814

- **SGI Advanced Linux Environment Multiple Updates**
  "Denial of Service"

  SGI has issued a patch for SGI Advanced Linux Environment. This fixes some vulnerabilities, which can be exploited by malicious people to cause a DoS (Denial of Service) or to compromise a vulnerable system.

  References:

ftp://patches.sgi.com/support/free/security/advisories/20050902-01-U.asc

- **Linux Kernel URB Handling Denial of Service Vulnerability**
  "Denial of Service"

  A vulnerability and a security issue have been reported in the Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

  1) An error in handling asynchronous USB access via usbdevio can be exploited to crash the kernel via a process that issues an URB (USB Request Block) from userspace and terminates before the URB returns.

  Successful exploitation requires that the user has permissions to access an USB device.

  2) An error in jiffies comparison in the "ipt_recent.c" netfilter module, when its value is greater than LONG_MAX, may cause ipt_recent netfilter rules to block too early.

  References:
  http://marc.theaimsgroup.com/?l=linux-kernel&m=112766129313883
  http://blog.blackdown.de/2005/05/09/fixing-the-ipt_recent-netfilter-module/

- **Sun Solaris Xsun and Xprt Privilege Escalation Vulnerability**
  "Gain escalated privileges"

  A vulnerability has been reported in Solaris, which can be exploited by malicious, local users to gain escalated privileges.

  The vulnerability is caused due to an unspecified error in the Xsun and Xprt commands. This can be exploited by unprivileged users to execute arbitrary code with the privileges of either command.

  The vulnerability has been reported in Solaris 7, 8, 9, and 10.

  References:
  http://sunsolve.sun.com/search/document.do?assetkey=1-26-101800-1

- **Microsoft Internet Explorer "XMLHTTP" HTTP Request Injection**
  "Manipulate certain data and conduct HTTP request smuggling attacks"

  Amit Klein has discovered a vulnerability in Microsoft Internet Explorer, which can be exploited by malicious people to manipulate certain data and conduct HTTP request smuggling attacks.

Input passed to the method parameter in the "open()" function in the "Microsoft.XMLHTTP" ActiveX control isn't properly sanitized before being used in a HTTP request. This can be exploited to inject arbitrary HTTP requests via specially crafted input containing tab and newline characters (spaces are not allowed).

Successful exploitation requires that the HTTP request is sent to a server or via a proxy allowing tab characters instead of spaces in certain parts of the HTTP request.

It has also been reported that the "referer" HTTP header can modified via the "SetRequestHeader()" function by appending a colon ":" to the header name (normally Internet Explorer does not allow the "referer" header to be changed).

The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2. Other versions may also be affected.

References:
http://secunia.com/advisories/16942/

❖ **SUN Solaris UFS File System Denial of Service**
"Denial of Service"

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

The vulnerability is caused due to an unspecified error in the UFS (Unix File System). This can be exploited by unprivileged users with "write" access to cause a "soft hang" of the system.

Successful exploitation requires that UFS logging is enabled.

The vulnerability has been reported in Solaris 8 and 9 on both SPARC and x86 platforms.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101940-1

❖ **Mac OS X Security Update Fixes Multiple Vulnerabilities**

Apple has issued a security update for Mac OS X, which fixes 10 vulnerabilities.

1) A boundary error in ImageIO can be exploited to cause a buffer overflow and may allow execution of arbitrary code on a user's system when a specially crafted GIF file is opened e.g. in WebCore or Safari.

2) An error in Mail.app when processing auto-reply rules can cause an automatically generated response message to include a plain-text copy of the encrypted message. This may disclose certain sensitive information.

3) An error in Mail.app when using Kerberos 5 for SMTP authentication can cause un-initialized memory to be appended to a message. This may disclose certain sensitive information. For Mac OS X v10.4.2, the vulnerability was fixed in Security Update 2005-007.

4) "malloc" creates diagnostic files insecurely when the "MallocLogFile" environment variable is set to enable logging when debugging application memory allocation. This can be exploited by malicious, local users to create or overwrite arbitrary files when running suid root applications.

5) A boundary error in QuickDraw Manager can be exploited to cause a buffer overflow and may allow arbitrary code execution on a user's system when a specially crafted PICT file is viewed e.g. from Safari, Mail, or Finder.

6) A validation error in the Java extensions bundled with QuickTime 6.52 and earlier can be exploited by untrusted applets to call arbitrary functions from system libraries. Systems with QuickTime 7 or later, or Mac OS X v10.4 or later, are not affected.

7) A vulnerability in Ruby can be exploited by malicious people to bypass certain security restrictions. Systems prior to Mac OS X v10.4 are not affected.

8) A validation error in Safari when rendering web archives from a malicious site can be exploited to execute arbitrary HTML and script code in a user's browser session in the context of another site. For Mac OS X v10.4.2, the vulnerability was fixed in Security Update 2005-007.

9) An error in the SecurityAgent may cause the "Switch User..." button to be displayed even when the "Enable fast user switching" setting has been disabled. This may allow malicious, local users to access the current user's desktop without authentication even when the "Require password to wake this computer from sleep or screen saver" setting is enabled.

10) A validation error in the Authorization Services "securityd" allows unprivileged users to gain certain privileges that should be restricted to administrative users. This can be exploited by malicious, local users to gain escalated privileges.

References:
http://docs.info.apple.com/article.html?artnum=302413
http://www.suresec.org/advisories/adv7.pdf

- **7-Zip ARJ Archive Handling Buffer Overflow**
  "Arbitrary code execution"

  Secunia Research has discovered a vulnerability in 7-Zip, which can be exploited by malicious people to compromise a user's system.

  The vulnerability is caused due to a boundary error when handling an ARJ block that is larger than 2600 bytes. This can be exploited to cause a stack-based buffer overflow when a specially crafted ARJ file is opened.

  Successful exploitation allows arbitrary code execution.

  The vulnerability has been confirmed in version 3.13, 4.23, and 4.26 BETA. Other versions may also be affected.

  http://secunia.com/secunia_research/2005-45/advisory/

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