netVigilance

ScoutNews Team **January 28th 2005**
Issue # 4

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

The return of the Bagle worm – sounds like a title for a hot encore movie. It's not, this time the Bagle worm is riding open source, and thus very dangerous for all those corporations that have based their IT infrastructure on open source tools.
Other places authorities are fighting back and showing that it will not pay off being an internet criminal. An E-Bay con man has been arrested and a young worm writer has been sentenced to jail.

Enjoy reading

New in SecureScout:
Improved Host Connectivity Check feature in SecureScout NX:

Disabling checks for the responsiveness of hosts on your network is more flexible in SecureScout NX now. Improvements to the user interface enable you to disable connectivity checks for ranges of IP addresses, your entire network as well as individual IP addresses. This greatly simplifies disabling ICMP / TCP port probes for targets that do not respond to normal probes like bastion hosts, Firewalls, DMZ hosts etc.

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

Top Security News Stories this Week

- **Man Accused in EBay Scandal Arrested**

A man is accused of selling almost $100,000 worth of Rolex watches and professional sports tickets on the Web site eBay, but never delivering the goods.
Gilbert Vartanian was arrested Thursday in the Sacramento suburb of Fremont on 12 counts of mail fraud.
Vartanian is accused of defrauding more than 10 victims of $93,324.52 between January 2001 and June 2004. He maintained at least three eBay accounts and more than a dozen user names, according to a federal grand jury indictment.
http://story.news.yahoo.com/news?tmpl=story&ncid=1212&e=10&u=/ap/20050128/a

p_on_hi_te/brf_ebay_arrest&sid=95573501
Associated Press

- **Man Sentenced for Releasing Computer Worm**

A teenager was sentenced Friday to 1 1/2 years in prison for unleashing an Internet worm that crippled 48,000 computers in 2003.
Jeffrey Lee Parson, 19, of Hopkins, Minn., will serve his time at a low-security prison and must also perform 10 months of community service.
He could have gotten 10 years behind bars, but the judge took pity on him, saying his neglectful parents were to blame for the psychological troubles that led to his actions.
http://story.news.yahoo.com/news?tmpl=story&ncid=1212&e=2&u=/ap/20050128/ap_on_hi_te/internet_attack&sid=95573501
Gene Johnson

- **Riding on Open Code, Bagle Worm Returns**

The Bagle worm is rearing its head again, back for another crack at the unprotected masses. There are likely two different variants that are new, experts said, though each respective security firm uses its own naming convention so the actual number of newly named variants across the different firms is greater. The latest variants have been labeled the Bagle.BJ virus (McAfee), W32/Bagle.bk@MM (McAfee and PandaLabs) Bagle.AY (F-Secure and Sophos), W32.Beagle.AZ@mm (Symantec), Win32.Bagle.ax (Kaspersky),WORM_BAGLE.AZ (Trend Micro), Win32.Bagle.AU (Computer Associates) and Bagle.BL (PandaLabs).
Many security firms have raised the threat level for the variants from moderate to severe or critical, as more instances of the rapidly spreading worm are reported. As is typical with variants of the Bagle family of worms, the polymorphic malicious code reaches user inboxes via a spoofed sender e-mail address, with a random subject line taken from a long list of choices and with random message content.
http://www.internetnews.com/dev-news/article.php/3465321
Sean Michael Kerner

New Vulnerabilities Tested in SecureScout

- **13182 Oracle Database Server - UTL_FILE component unspecified error (jan-2005/DB04)**

An unspecified error in the UTL_FILE component can potentially be exploited to manipulate information.

Successful exploitation requires permissions to read on a database directory object.

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

CVE Links:

Reference: http://www.oracle.com/technology/deploy/security/pdf/cpu-jan-2005_advisory.pdf & http://www.oracle.com/

- **13183 Oracle Database Server - Diagnostic component unspecified error (jan-2005/DB05)**

An unspecified error in the Diagnostic component can potentially be exploited to disclose information, manipulate data, or cause a DoS.

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

CVE Links:

Reference: http://www.oracle.com/technology/deploy/security/pdf/cpu-jan-2005_advisory.pdf & http://www.oracle.com/

- **13184 Oracle Database Server - XDB component unspecified error (jan-2005/DB06)**

An unspecified error in the XDB component can potentially be exploited to disclose or manipulate information.

Successful exploitation requires execute permissions on the xdb.dbms_xdb packages.

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

CVE Links:

Reference: http://www.oracle.com/technology/deploy/security/pdf/cpu-jan-2005_advisory.pdf & http://www.oracle.com/

- **13185 Oracle Database Server - XDB component unspecified error (jan-2005/DB07)**

Two unspecified errors in the XDB component can potentially be exploited to disclose or manipulate information.

Successful exploitation requires execute permissions on the xdb.dbms_xdbz0 package.

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

CVE Link:

Reference: http://www.oracle.com/technology/deploy/security/pdf/cpu-jan-2005_advisory.pdf & http://www.oracle.com/

- **13186 Oracle Database Server - XDB component unspecified error (jan-2005/DB08)**

Two unspecified errors in the XDB component can potentially be exploited to disclose or manipulate information.

Successful exploitation requires execute permissions on the xdb.dbms_xdbz0 package.

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

CVE Link:

Reference: http://www.oracle.com/technology/deploy/security/pdf/cpu-jan-

2005_advisory.pdf & http://www.oracle.com/

- **13187 Oracle Database Server - Dataguard component unspecified error (jan-2005/DB09)**

  An unspecified error in the Dataguard component can potentially be exploited to disclose or manipulate information.

  Successful exploitation requires execute permissions on the exfsys.dbms_expfil package.

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

CVE Link:

Reference: http://www.oracle.com/technology/deploy/security/pdf/cpu-jan-2005_advisory.pdf & http://www.oracle.com/

- **13188 Oracle Database Server - Log Miner component unspecified error (jan-2005/DB10)**

  An unspecified error in the Log Miner component can potentially be exploited to disclose or manipulate information.

  Successful exploitation requires execute permissions on the dbms_logmnr package.

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

CVE Link:

Reference: http://www.oracle.com/technology/deploy/security/pdf/cpu-jan-2005_advisory.pdf & http://www.oracle.com/

- **13189 Oracle Database Server - OLAP component unspecified error (jan-2005/DB11)**

  An unspecified error in the OLAP component can potentially be exploited to disclose or manipulate information.

  Successful exploitation requires execute permissions on the olapsys package.

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

CVE Link:

Reference: http://www.oracle.com/technology/deploy/security/pdf/cpu-jan-2005_advisory.pdf & http://www.oracle.com/

- **13190 Oracle Database Server - Data Mining component unspecified error (jan-2005/DB12)**

  An unspecified error in the Data Mining component can potentially be exploited to disclose or manipulate information.

Successful exploitation requires execute permissions on the dmsys.dmp_sys package.

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

CVE Link:

Reference: http://www.oracle.com/technology/deploy/security/pdf/cpu-jan-2005_advisory.pdf & http://www.oracle.com/

- **13191 Oracle Database Server - Advanced Queuing component unspecified error (jan-2005/DB13)**

An unspecified error in the Advanced Queuing component can potentially be exploited to disclose or manipulate information.

Successful exploitation requires execute permissions on the dbms_transform_eximp package.

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

CVE Link:

Reference: http://www.oracle.com/technology/deploy/security/pdf/cpu-jan-2005_advisory.pdf & http://www.oracle.com/

New Vulnerabilities found this Week

- **Juniper JUNOS Unspecified Packet Processing Denial of Service**

"Denial of Service"

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

The vulnerability is caused due to an unspecified error within the processing of certain network packets. This can be exploited to disrupt the operation of a vulnerable device via some specially crafted network packets.

The vulnerability affects all releases of JUNOS built prior to 2005-01-07.

References:
https://www.juniper.net/alerts/viewalert.jsp?txtAlertNumber=PSN-2005-01-009&actionBtn=Search
http://www.kb.cert.org/vuls/id/409555

- **Sun Solaris UDP End Point Handling Denial of Service**

"Denial of Service"

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

The vulnerability is caused due to an error in the handling of UDP end points. This may be

exploited to crash a vulnerable system by opening and closing multiple UDP end points.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57728-1

- **Cisco IOS BGP Protocol Processing Denial of Service**

"Denial of Service"

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

The vulnerability is caused due to an error within the handling of queued BGP (Border Gateway Protocol) packets when logging a BGP neighbor change. This can be exploited to cause a vulnerable device to reload by sending a specially crafted BGP packet, which seems to originate from a configured, trusted peer.

Successful exploitation requires enabled BGP support and the command "bgp log-neighbor-changes" configured.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml
http://www.kb.cert.org/vuls/id/689326

- **Cisco IOS IPv6 Packet Processing Denial of Service**

"Denial of Service"

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

The vulnerability is caused due to an error within the processing of IPv6 packets. This can be exploited to cause a vulnerable device to reload via multiple specially crafted IPv6 packets.

Successful exploitation requires that the device has been configured to process IPv6 traffic.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml
http://www.kb.cert.org/vuls/id/472582

- **Cisco IOS MPLS Packet Processing Denial of Service**

"Denial of Service"

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

The vulnerability is caused due to an error within the processing of MPLS (Multi Protocol Label Switching) packets. This can be exploited to cause a vulnerable device to reload by sending a specially crafted MPLS packet to an interface with MPLS disabled.

Successful exploitation requires support for MPLS; however, it does not have to be configured.

The vulnerability affects the following products with release trains based on 12.1T, 12.2, 12.2T, 12.3, and 12.3T:
* 2600 and 2800 series routers
* 3600, 3700 and 3800 series routers
* 4500 and 4700 series routers
* 5300, 5350 and 5400 series Access Servers

References:
http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml
http://www.kb.cert.org/vuls/id/583638

- **Sun Solaris DHCP Administration Utilities Vulnerability**

"Gain escalated privileges"

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

The vulnerability is caused due to unspecified errors in the DHCP administration utilities (dhcpconfig, pntadm, and dhcpmgr).

Successful exploitation allows execution of arbitrary code with root privileges.

The vulnerability affects the following versions:
* Solaris 8 with patch 109077-02 through 109077-08 and without patch 109077-09 (SPARC platform)
* Solaris 8 with patch 109078-02 through 109078-08 and without patch 109078-09 (x86 platform)

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57727-1

- **Evolution camel-lock-helper Integer Overflow Vulnerability**

"Gain escalated privileges"

Max Vozeler has reported a vulnerability in Evolution, which can be exploited by malicious people to compromise a user's system and by malicious, local users to gain escalated privileges.

The vulnerability is caused due to an integer overflow in camel-lock-helper application. This can be exploited by a malicious, local user or POP3 server to cause a buffer overflow and execute arbitrary code with the privileges of the camel-lock-helper application.

References:
http://www.ubuntulinux.org/support/documentation/usn/usn-69-1
http://security.gentoo.org/glsa/glsa-200501-35.xml

- **SquirrelMail Three Vulnerabilities**

"Cross-site scripting attacks"

Three vulnerabilities have been reported in SquirrelMail, which can be exploited by malicious people to gain knowledge of sensitive information or conduct cross-site scripting attacks.

1) Insufficient sanitation of integer variables in webmail.php can be exploited to include arbitrary HTML and script code, which will be executed in a user's browser session in context of an affected site.

The vulnerability affects versions 1.4.0-RC1 through 1.4.4-RC1.

2) Insufficient validation of incoming URL vars in webmail.php can be exploited to include arbitrary web pages in the SquirrelMail frameset.

The vulnerability affects versions 1.4.0-RC1 through 1.4.4-RC1.

3) An error in prefs.php can be exploited to include arbitrary code from local resources via a specially crafted URL.

Successful exploitation requires that register_globals is set to "On".

The vulnerability affects versions 1.4.3-RC1 through 1.4.4-RC1.

References:
http://www.squirrelmail.org/security/issue/2005-01-20
http://www.squirrelmail.org/security/issue/2005-01-19
http://www.squirrelmail.org/security/issue/2005-01-14

- **OpenH323 Gatekeeper Multiple Sockets Buffer Overflow**

“Denial of Service”

A vulnerability has been reported in OpenH323 Gatekeeper, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to a missing boundary check when doing "FD_SET()" operations. This can be exploited to cause a buffer overflow in certain configurations by establishing multiple concurrent connections.

The vulnerability has been reported in version 2.2.0. Prior versions may also be affected.

References:
http://www.security.nnov.ru/advisories/sockets.asp

- **Ethereal Multiple Unspecified Packet Dissector Vulnerabilities**

“Denial of Service”

Multiple vulnerabilities have been reported in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service) or potentially compromise a vulnerable system.

1) An unspecified error in the COPS dissector can be exploited to cause the process to enter an infinite loop and consume available CPU resources.

The vulnerability affects versions 0.10.6 through 0.10.8.

2) An unspecified error in the DLSw dissector can be exploited to crash the process.

The vulnerability affects versions 0.10.6 through 0.10.8.

3) An unspecified error in the DNP dissector can be exploited to corrupt memory content.

The vulnerability affects versions 0.10.5 through 0.10.8.

4) An unspecified error in the Gnutella dissector can be exploited to crash the process.

The vulnerability affects versions 0.10.6 through 0.10.8.

5) An unspecified error in the MMSE dissector may cause it to free static memory.

The vulnerability affects versions 0.10.4 through 0.10.8.

6) A boundary error in the X11 dissector can be exploited to cause a buffer overflow and potentially execute arbitrary code.

The vulnerability affects versions 0.8.10 through 0.10.8.

References:
http://www.ethereal.com/appnotes/enpa-sa-00017.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