netVigilance

ScoutNews Team

February 4 2005
Issue # 5

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Kevin Mitnick illustrates how cyber crime has exploded and will only continue to grow and new trend in Spammers hijacking ISP mail servers to act as ‘Zombies’ to proliferate Spam.

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

- **Mitnick Speaks**

From hijacked PCs that spew spam to denial-of-service attacks that crash Web servers, cyber-crime means billions of dollars a year in lost revenues and productivity. And no computer user is safe. “It’s not if,” says Kevin Mitnick, “it’s when are you going to get hacked.”

Last fall, Mitnick along with Avantgarde, a tech marketing and design firm in San Francisco, hooked up six computer platforms to the Internet via broadband DSL and recorded the cyber-attacks that occurred over a two-week period. It took less than four minutes for an automated attack to successfully break through the security defenses of one newly connected PC; most machines without an active firewall faced more than 300 attacks per hour, while those with firewall protection faced fewer than four per hour.

Full story:
http://www.technologyreview.com/articles/05/03/issue/forward_hacker.asp
Technology Review.com

- **Spammers hijacking ISP mail servers to bypass anti-spam filters.**

SPAM served fresh from your own ISP completely avoids anti-spam filters and content filtering. Savvy hackers enlist ISP mail servers to deliver SPAM, coming from trusted source; Spam filters are not effective.

SPAM now constitutes 75% of all email traffic; more sophisticated Spamming methods could drive this figure to 95% according to Spamhaus.

ISP's need to take added measures to prevent becoming leading Spam sources, like proactively securing mail servers from intrusion.

http://www.spamhaus.org/news.lasso?article=156
Spamhaus.org

New Vulnerabilities Tested in SecureScout

- **13192 Oracle Database Server - Change Data Capture component unspecified error (jan-2005/DB14)**

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

  Successful exploitation requires execute permissions on the dbms_cdc_dputil package.

  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

- **13193 Oracle Database Server - Change Data Capture component unspecified error (jan-2005/DB15)**

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

  Successful exploitation requires execute permissions on the dbms_cdc_impdp package.

  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/

- **13194 Oracle Database Server - Database Core component component unspecified error (jan-2005/DB16)**

  An unspecified error in the Database Core component can be exploited to disclose or manipulate information.

  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/

- **13195 Oracle Database Server - XDB component unspecified error (jan-2005/DB07)**
  An unspecified error in the OHS component can potentially be exploited to disclose or manipulate information.

  Successful exploitation requires execute permissions on the owa_opt_lock 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/

- **15159 ISC BIND "q_usedns" Array Buffer Overflow Vulnerability**
  Advisory Copyright: Internet Software Consortium

  ISC BIND 8.4.4 and 8.4.5 allows remote attackers to perform a DoS attack.
  Test
  Case Impact: **Gather Info** Vulnerability Impact: **DOS** Risk: **Medium**

  CVE Link: CAN-2005-0033

  Reference: http://www.kb.cert.org/vuls/id/327633, http://www.isc.org/sw/bind/bind-security.php

15160 ISC BIND Validator Denial of Service Vulnerability
A vulnerability has been reported in BIND, which can be exploited by

malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the validator within the "authvalidated()" function and may result in an internal consistency test failing when processing a specially crafted DNS datagram.

Successful exploitation causes named to exit, but requires that DNSSEC validation is enabled (not default setting).

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

CVE Link: CAN-2005-0034

Reference: http://www.kb.cert.org/vuls/id/938617, http://www.isc.org/index.pl?/sw/bind/bind-security.php

15575 Cisco IOS BGP Protocol Processing Denial of Service Vulnerability (CSCee67450)

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

The vulnerability is caused due to an error in the validator within the "authvalidated()" function and may result in an internal consistency test failing when processing a specially crafted DNS datagram.

Successful exploitation causes named to exit, but requires that DNSSEC validation is enabled (not default setting).

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

CVE Link:

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

❖ 15576 Cisco IOS IPv6 Packet Processing Denial of Service Vulnerability (CSCee67450)

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.

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

CVE Link:

Reference: http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml, http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml#software

- **15577 Cisco IOS MPLS Packet Processing Denial of Service Vulnerability (CSCee67450)**
  A vulnerability has been reported in Cisco IOS, which can be exploited by malicious people to cause a DoS (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.

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

  CVE Link:

  Reference: http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml, http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml#software

- **17931 SquirrelMail PHP File Inclusion and XSS Vulnerabilities**
  A vulnerability has been reported in Cisco IOS, which can be exploited by malicious people to cause a DoS (Denial of Service).

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

  CVE Link:

  Reference: http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml, http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml#software

New Vulnerabilities found this Week

- **Eudora email vulnerabilities enable malicious code attacks.**

"Malicious Code"

John Heasman of NGSSoftware has reported some vulnerabilities in Eudora, which can be exploited by malicious people to compromise a user's system.

The vulnerabilities are caused due to unspecified errors within the viewing of emails and handling of stationary and mailbox files.

Successful exploitation allows execution of arbitrary code with the privileges of the user running Eudora. The vulnerabilities have been reported in versions 6.2.0 and prior for Windows.

References:

http://www.eudora.com/security.html

❖ W32/Bropia.worm.g

"Denial of Service, Unauthorized Access"

As with the multitude of other W32/Sdbot.worm variants, this one bears the following characteristics (the list is not exhaustive, just representative of some of the functionality the bot provides to the hacker):

enables remote command to spawn functionality such as:

- Institute proxy for Spam, other attacks
- denial of service attack against remote machines
- run keylogger on victim machine
- harvest data from victim machine (ie: passwords, keys, browse/kill/start/pause running processes

References:
http://secunia.com/virus_information/15107/bropia.f/

❖ Sun Solaris Samba Integer Overflow Vulnerability

"Malicious Code"

Sun has acknowledged a vulnerability in Solaris, which can be exploited by malicious users to compromise a vulnerable system.

The vendor recommends downloading and compiling Samba 3.0.10 or higher from Samba.org. A final resolution is reportedly pending completion.

References:
http://secunia.com/advisories/14130/
http://us1.samba.org/samba/ftp/p.../samba-3.0.9-CAN-2004-1154.patch
CAN-2004-1154

- **Savant Web Server 3.1 Remote Buffer Overflow**

"Root Access"

Exploit for Remote Buffer overflow on Savant Web Server 3.1 has been published for Windows 2003.

References:
http://www.securityfocus.com/archive/1/389512/2005-02-01/2005-02-07/0

- **HP CIFS Server Security Descriptor Parsing Integer Overflow**

"System Access"

HP has acknowledged a vulnerability in CIFS Server, which can be exploited by malicious users to compromise a vulnerable system.

References:
http://secunia.com/advisories/14132/
http://software.hp.com/

- **Crafted Packet Causes Reload on Cisco Routers**

"Denial of Service"

Cisco Routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on interfaces where MPLS is not configured. A system that supports MPLS is vulnerable even if that system is not configured for MPLS.
The vulnerability is only present in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable.
Cisco has made free software available to address this vulnerability.
There are workarounds available to mitigate the effects.

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

- **Security Vulnerability in Solaris 8 DHCP Administration Utilities**

"Privilege Escalation"

A security vulnerability in the DHCP administration utilities dhcpconfig(1M), pntadm(1M), and dhcpmgr(1M) may allow an unprivileged local user the ability to execute arbitrary code with the privileges of root.

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

- **Ubuntu 4.10 evolution buffer overflow**

"Root Access"

An user-supplied length value was not validated, so that a value of -1 caused a buffer allocation of 0 bytes; this buffer was then filled by an arbitrary amount of user-supplied data.

A local attacker or a malicious POP3 server could exploit this to execute arbitrary code with root privileges (because camel-lock-helper is installed as setuid root).

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

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