netVigilance

ScoutNews Team

April 15, 2005
Issue # 15

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Toxic Blogs, triumph of the worm, 'tagging' of the Anchorage Airport website and conduct your web-conferencing and telecommuting with care.

netVigilance is officially blessed as CVE compatible. As you have noticed; netVigilance has always included CVE references in our testcase descriptions and have CVE-specific policy definitions.

Well now it's official. Mitre CVE has finished testing of SecureScout and given it the CVE-compatible stamp of approval. Read more here: http://www.cve.mitre.org/

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

- **Kelvir-U delivers Knock-Out punch to Reuters IM service.**

An MSN worm known as Kelvir-U infected Reuters, forcing a shutdown of MSN and Windows Messaging services; affecting roughly 60,000 users.

The worm baits users into clicking on a url that in turn installs the Spybot worm to glean the user's contacts list and further spread itself. Spybot usually opens a backdoor to be used for future attacks.

The worm could have entered the network via email or instant messaging.
The Register / eweek

More on this story:
http://www.eweek.com/article2/0,1759,1786152,00.asp
http://www.theregister.co.uk/2005/04/15/im_worm_runs_amok/

❖ Beware of Toxic blogs spreading malware.

Hackers are using illegitimate and legitimate Blog sites to store and propagate malware such as Keyloggers and Trojans.

Most legitimate Blog sites provide some amount of free storage. Hackers are taking advantage of this generosity to hide their malicious code and pass to unsuspecting visitors. Common sense and caution are the user's only defense. Be suspicious of executables and urls appearing in Blog site messages; these are being used as the first steps in blended attacks.
ComputerWeekly.com

Related Links :
http://www.techweb.com/wire/ebiz/160702361

http://www.computerweekly.com/articles/article.asp?liArticleID=137915&liArticleTypeID=1&liCategoryID=2&liChannelID=22&liFlavourID=1&sSearch=&nPage=1

❖ Anchorage International Airport hacked; site down for over 8 hours.

A Turkish hacker who goes by the handle "iSKORPiTX", broke into the Web site of the Ted Stevens Anchorage International Airport and replaced Arrival / Departure information with an image of a waving Turkish flag.

This represents a growing trend in cyber attacks being launched from relatively un-policed regions of the world like the former Soviet Bloc states and the increasingly connected parts of E. Asia.

Cybervandalism; while relatively harmless, is usually a prelude to cyberpunks graduating to serious criminal actions; putting their nefarious skills to work in committing theft in order to finance their activities.

USA Today

Full Story:
http://www.usatoday.com/travel/news/2005-04-13-ala-airport-hacking_x.htm?csp=34

- **UK report cite home workers as security risk.**

Novell found 80% of Britons admit to not taking computer security precautions when working from home.

Telecommuting is on the rise worldwide; so the solution is to implement policies and practices that extend the corporate security posture to the remote employee.

Related Stories:
http://news.bbc.co.uk/2/hi/uk_news/4446827.stm

- **Web-conferencing, getting more popular – opens vulnerabilities.**

Corporations looking to enable quicker decision-making and cut expenses, are tuning more and more to web-conferencing. Revenues for web-conferencing services grew 40% from ’02 to ’04.

Web-conferencing requires that vital information be shared outside of the firewall and is dependent on 3-party applications and servers that contain vulnerabilities.

Be sure to shop carefully for your web-conferencing solution. Security, even at the expense of bandwidth, should be your gating factor.

Related Link:
http://www.computer.org/computer/homepage/0205/trends/index.htm

New Vulnerabilities Tested in SecureScout

❖ 13212 Oracle Database Server - Change Data Capture component unspecified error (apr-2005/DB01)

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

Successful exploitation requires execute permissions on DBMS_CDC_IPUBLISH.

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

References:

Original Advisory:

http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf

http://www.ngssoftware.com/advisories/oracle-03.txt

http://secunia.com/advisories/14935/

Product Homepage:

http://www.oracle.com/

CVE Reference: None.

❖ 13213 Oracle Database Server - Change Data Capture component unspecified error (apr-2005/DB02)

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

Successful exploitation requires execute permissions on DBMS_CDC_{I}SUBSCRIBE.

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

References:

Original Advisory:

http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf

http://www.ngssoftware.com/advisories/oracle-03.txt

http://secunia.com/advisories/14935/

Product Homepage:

http://www.oracle.com/

CVE Reference: None.

❖ 14703 Vulnerability in Windows Shell that Could Allow Remote Code Execution (MS05-016/893086) (Remote File Checking)

A remote code execution vulnerability exists in the Windows Shell because of the way that it handles application association. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of the affected system. However, user interaction is required to exploit this vulnerability.

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

References:

http://www.microsoft.com/technet/security/bulletin/MS05-016.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0063

CVE Reference: CAN-2005-0063

❖ 14704 Vulnerability in Message Queuing Could Allow Code Execution (MS05-017/892944) (Remote File Checking)

A remote code execution vulnerability exists in Message Queuing that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

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

References:

http://www.microsoft.com/technet/security/bulletin/MS05-017.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0059

CVE Reference: CAN-2005-0059

❖ 14705 Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege and Denial of Service (MS05-018/890859) (Remote File Checking)

A privilege elevation vulnerability exists in the way that Windows process certain fonts. This vulnerability could allow a logged on user to take complete control of the system.

A privilege elevation vulnerability exists in the way that the affected operating system versions process certain access requests. This vulnerability could allow a logged on user to take complete control of the system.

A denial of service vulnerability exists that could allow an attacker to send a specially crafted request locally to an affected operating system version. An attacker who exploited this vulnerability could cause the affected system to stop responding and automatically restart

A privilege elevation vulnerability exists in the way that the affected operating system versions process certain access requests. This vulnerability could allow a logged on user to take complete control of the system.

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

References:

http://www.microsoft.com/technet/security/bulletin/MS05-018.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0060
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0061
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0550
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-055

CVE Reference: CAN-2005-0060 CAN-2005-0061 CAN-2005-0550 CAN-2005-0551

❖ 14706 Vulnerabilities in TCP/IP Could Allow Remote Code Execution and Denial of Service (MS05-019/893066) (Remote File Checking)

A remote code execution vulnerability exists that could allow an attacker to send a specially crafted IP message to an affected system. An attacker who successfully exploited this vulnerability could cause the affected system to remotely execute code. However, attempts to exploit this vulnerability would most likely result in a denial of service.

A denial of service vulnerability exists that could allow an attacker to send a specially crafted Internet Control Message Protocol (ICMP) message to an affected system. An attacker who successfully exploited this vulnerability could cause the affected system to reset existing TCP connections.

A denial of service vulnerability exists that could allow an attacker to send a specially crafted Internet Control Message Protocol (ICMP) message to an affected system that could cause network performance to degrade and potentially stop the affected system from responding to requests.

A denial of service vulnerability exists that could allow an attacker to send a specially crafted TCP message to an affected system. An attacker who successfully exploited this vulnerability could cause the affected system to reset existing TCP connections.

A denial of service vulnerability exists that could allow an attacker to send a specially crafted TCP/IP message to an affected system. An attacker who successfully exploited this vulnerability could cause the affected system to stop responding.

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

References:

http://www.microsoft.com/technet/security/bulletin/MS05-019.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0048
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0790
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1060
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0230
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-068

CVE Reference: CAN-2005-0048 CAN-2004-0790 CAN-2004-1060 CAN-2004-0230 CAN-2005-0688

❖ 14707 Cumulative Security Update for Internet Explorer (MS05-020/890923) (Remote File Checking)

A remote code execution vulnerability exists in Internet Explorer because of the way that it handles certain DHTML objects. An attacker could exploit the vulnerability by constructing a malicious Web page. This malicious Web page could allow remote code execution if a user visited a malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A remote code execution vulnerability exists in Internet Explorer because of the way that it handles certain URLs. An attacker could exploit the vulnerability by constructing a malicious Web page. This malicious Web page could potentially allow remote code execution if a user visited a malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A remote code execution vulnerability exists in Internet Explorer because of the way that it handles Content Advisor files. An attacker could exploit the vulnerability by constructing a specially crafted Content Advisor file. This malicious Content Advisor file could potentially allow remote code execution if a user visited a malicious Web site or viewed a malicious e-mail message and accepted the installation of the file. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, significant user interaction is required to exploit this vulnerability.

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

References:

http://www.microsoft.com/technet/security/bulletin/MS05-020.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0553
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0554
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0555

CVE Reference: CAN-2005-0553 CAN-2005-0554 CAN-2005-0555

❖ 14708 Vulnerability in Exchange Server Could Allow Remote Code Execution (MS05-021/894549) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Exchange Server that that could allow an attacker to connect to the SMTP port on an Exchange server and issue a specially-crafted command that could result in a denial of service or allow an attacker to run malicious programs of their choice in the security context of the SMTP service.

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

References:

http://www.microsoft.com/technet/security/bulletin/MS05-021.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0560

CVE Reference: CAN-2005-0560

❖ 14709 Vulnerability in MSN Messenger Could Lead to Remote Code Execution (MS05-022/896597) (Remote File Checking)

A remote code execution vulnerability exists in MSN Messenger that could allow an attacker who successfully exploited this vulnerable to take complete control of the affected system.

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

References:

http://www.microsoft.com/technet/security/bulletin/MS05-022.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0562

CVE Reference: CAN-2005-0562

❖ 14710 Vulnerabilities in Microsoft Word May Lead to Remote Code Execution (MS05-023/890169) (Remote File Checking)

A vulnerability exists in Microsoft Word that could allow an attacker to run arbitrary code on a users system.
If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges.
Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

A vulnerability exists in Microsoft Word that could allow an attacker to run arbitrary code on a users system.
If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges.
Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

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

References:

http://www.microsoft.com/technet/security/bulletin/MS05-023.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0963
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0558

CVE Reference: CAN-2004-0963 CAN-2005-0558

New Vulnerabilities found this Week

❖ Sun Java System Web Server Unspecified Denial of Service "Denial of Service"

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

The vulnerability is caused due to an unspecified error and can be exploited to cause the web server to become unresponsive.

The vulnerability affects Sun Java System Web Server 6.0 Service Pack 7 and prior for Windows.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57760-1

❖ Sun Java System Directory Server LDAP Request Buffer Overflow “Denial of Service”

Sun has acknowledged a vulnerability in Sun ONE/Java System Directory Server, which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the access control implementation when handling LDAP requests. This can be exploited to cause a buffer overflow via a specially crafted, invalid LDAP request.

Successful exploitation crashes the LDAP service or allows execution of arbitrary code with the privileges of the LDAP process.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57754-1
http://www.kb.cert.org/vuls/id/258905

❖ Sun Solaris ICMP Message Handling Denial of Service “Denial of Service”

Sun has acknowledged some security issues in Solaris, which can be exploited by malicious people to cause a DoS (Denial of Service).

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57746-1

Oracle Products Multiple Unspecified Vulnerabilities
“Denial of Service”

Multiple vulnerabilities have been reported in various Oracle products. Some have an unknown impact, and others can be exploited to gain knowledge of sensitive information, manipulate data, or cause a DoS (Denial of Service).

The following supported products are affected by one or more vulnerabilities:
* Oracle Database 10g Release 1, versions 10.1.0.2, 10.1.0.3, 10.1.0.3.1, 10.1.0.4.
* Oracle9i Database Server Release 2, versions 9.2.0.5, 9.2.0.6
* Oracle9i Database Server Release 1, versions 9.0.1.4, 9.0.1.5, 9.0.4 (9.0.1.5 FIPS)
* Oracle8i Database Server Release 3, version 8.1.7.4
* Oracle Application Server 10g Release 2 (10.1.2)
* Oracle Application Server 10g (9.0.4), versions 9.0.4.0, 9.0.4.1
* Oracle9i Application Server Release 2, versions 9.0.2.3, 9.0.3.1
* Oracle9i Application Server Release 1, version 1.0.2.2
* Oracle Collaboration Suite Release 2, versions 9.0.4.1, 9.0.4.2
* Oracle E-Business Suite and Applications Release 11i, versions 11.5.0 through

11.5.10
* Oracle E-Business Suite and Applications Release 11.0
* Oracle Enterprise Manager Grid Control 10g, versions 10.1.0.2, 10.1.0.3
* Oracle Enterprise Manager versions 9.0.4.0, 9.0.4.1
* PeopleSoft EnterpriseOne Applications, versions 8.9 SP2 and 8.93
* PeopleSoft OneWorldXe/ERP8 Applications, versions SP22 and higher

NOTE: Consult the original vendor advisory for a vulnerability matrix detailing affected components, requirements, and impact.

References:
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
http://www.ngssoftware.com/advisories/oracle-03.txt

- **OpenOffice ".doc" Document Handling Buffer Overflow**
  “Execution of arbitrary code”

AD-LAB has reported a vulnerability in OpenOffice, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the "StgCompObjStream::Load()" function when processing ".doc" document files. This can be exploited to cause a heap-based buffer overflow by tricking a user into opening a malicious document containing a specially crafted header.

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been reported in versions 1.1.4 and prior and in the 2.0 beta release.

References:
http://www.openoffice.org/issues/show_bug.cgi?id=46388

- **Cisco Various Products ICMP Message Handling Denial of Service**
  “Denial of Service”

Fernando Gont has published an Internet-Draft describing how ICMP (Internet Control Message Protocol) can be exploited by malicious people to cause a DoS (Denial of Service). Cisco has acknowledged that various Cisco products are affected.

The published Internet-Draft details three types of attacks, which utilize the following ICMP messages to cause a negative impact on TCP connections either terminating or originating from a vulnerable device.

1) ICMP "hard" error messages
2) ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages

(known as PMTUD attacks)
3) ICMP "source quench" messages

These attacks can all be exploited to cause TCP connection resets, reduce the throughput in existing TCP connections, or consume large amounts of CPU and memory resources.

Successful exploitation requires knowledge of IP address information of the source and destination of the TCP network connection..

NOTE: See the original advisory for a list of affected versions.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml
http://www.niscc.gov.uk/niscc/docs/al-20050412-00308.html
http://www.gont.com.ar/drafts/icmp-attacks-against-tcp.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