netVigilance

ScoutNews Team **July 22, 2005**
Issue # 29

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Cyber crime losses drop; attacks on the rise, over 2/3 of internet traffic is malicious, the end of the perimeter Firewall? CardSystems looses BIG customers as a result of loose security.

Be careful and 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

- **FBI reports cyber-crime losses down**

A CSI/FBI Computer Crime and Security Survey produced by Computer Security Institute (CSI) and San Francisco FBI's Computer Intrusion Squad, reports that losses from cyber crime are down but attacks are on the increase.

A decrease in Virus attacks accounted for the big drop. This may indicate a trend where cyber criminals are interested in more than simply causing mischief. There were increases in damages associated with unauthorized access and theft of proprietary information shot up 488% and 111% respectfully.

Full Story:
http://www.esecurityplanet.com/trends/article.php/3521326

- **69% of Internet activity involves criminal intent, says report**

In a study commissioned by McAfee, the Centre for Strategic and International Studies in Washington, D.C. reports that cyber-criminals are aggressively staying ahead of network security developments to perpetrate all kinds of crimes including extortion, damage to reputation, fraud, Denial of Service and information theft.

Business Edge

Full Story :

http://www.businessedge.ca/article.cfm/newsID/10118.cfm

- **… and the [Fire]walls came tumbling down.**

In a trend that they have called 'de-perimeterisation', the Jericho Forum touts a new security architecture where perimeter firewalls are obsolete. The reasoning: they say it hinders e-commerce. An interesting idea, however amongst talks of increased threat levels and thin-client models, this does seem to be a voice from the wilderness.

Source

Related Links:
http://www.networkworld.com/news/2005/070405perimeter.html
http://www.opengroup.org/jericho/

- **CardSystems looses Visa, Amex due to data loss.**

In addition to mounting fines and lawsuits; CardSystems can add to their list of woes the loss of two of their primary customers. Quite possibly the most recognized logo worldwide; Visa alone made up over half of their business with the data processing house. MasterCard has given CardSystems until August 31st to meet data security standards.

RedHerring

Full Story:
http://www.redherring.com/Article.aspx?a=12823&hed=Credit+Cards+Bar+CardSystems&sector=Industries&subsector=SecurityAndDefense

New Vulnerabilities Tested in SecureScout

- `13263  Oracle Database Server - Oracle OLAP component Unspecified error (jul-2005/DB02)`

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

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujul2005.html

Product Homepage:
http://www.oracle.com/

CVE Reference: None

❖ **13264 Oracle Database Server - Component Registry component Unspecified error (jul-2005/DB03)**

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

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujul2005.html

Product Homepage:
http://www.oracle.com/

CVE Reference: None

❖ **13265 Oracle Database Server - CORE component Unspecified error (jul-2005/DB04)**

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

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujul2005.html

Product Homepage:
http://www.oracle.com/

CVE Reference: None

❖ **13266 Oracle Database Server - CORE component Unspecified error (jul-2005/DB05)**

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

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujul2005.html

Product Homepage:
http://www.oracle.com/

CVE Reference: None

❖ **13267 Oracle Database Server - XML Database component Unspecified error (jul-2005/DB06)**

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

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujul2005.html

Product Homepage:
http://www.oracle.com/

CVE Reference: None

❖ **13268 Oracle Database Server - XML Database component Unspecified error (jul-2005/DB07)**

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

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujul2005.html

Product Homepage:
http://www.oracle.com/

CVE Reference: None

❖ **13269 Oracle Database Server - iSQL*Plus component Unspecified error (jul-2005/DB08)**

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

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpujul2005.html

Product Homepage:
http://www.oracle.com/

CVE Reference: None

❖ **15652 Vulnerability in Microsoft Word Could Allow Remote Code Execution (MS05-035/903672) (Remote File Checking)**

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

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

http://www.microsoft.com/technet/security/Bulletin/MS05-035.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0564

CVE Reference: CAN-2005-0564

❖ **15653 Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution (MS05-036/901214) (Remote File Checking)**

A remote code execution vulnerability exists in the Microsoft Color Management Module because of the way that it handles ICC profile format tag validation. An attacker could exploit the vulnerability by constructing a malicious image file that could potentially allow remote code execution if a user visited a malicious Web site or viewed a malicious e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

http://www.microsoft.com/technet/security/Bulletin/MS05-036.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1219

CVE Reference: CAN-2005-1219

❖ **15654 Vulnerability in JView Profiler Could Allow Remote Code Execution (MS05-037/903235) (Remote File Checking)**

A remote code execution vulnerability exists in JView Profiler. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited the malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

http://www.microsoft.com/technet/security/Bulletin/MS05-037.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2087

CVE Reference: CAN-2005-2087

New Vulnerabilities found this Week

- **Sun Solaris gzip Directory Traversal Vulnerability**
  "Files to be extracted to an arbitrary directory"

Sun Microsystems has acknowledged a vulnerability in Solaris, which can be exploited by malicious people to cause files to be extracted to an arbitrary directory on a user's system.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101816-1

- **FreeBSD devfs Ruleset Bypass Security Issue**
  "Bypass certain security restrictions"

A security issue has been reported in FreeBSD, which can be exploited by malicious, local users to bypass certain security restrictions.

The security issue is caused due to insufficient checking of device node types during creation, which allows users or malicious code to access hidden "/dev" nodes within jailed processes with their normal access permissions. Jailed processes running with administrative privileges can potentially access all devices on the system.

The security issue has been reported in all FreeBSD 5.x releases.

References:
ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:17.devfs.asc

- **zlib Denial of Service Vulnerability**
  "Denial of Service"

Markus Oberhumer has reported a vulnerability in zlib, which can be exploited by malicious people to cause a DoS (Denial of Service) against a vulnerable application.

The vulnerability is caused due to the insufficient size of the code table declared in inflate.h, and can be exploited to cause an application using the zlib library to crash via a specially crafted input file.

The vulnerability has been reported in version 1.2.2. Prior versions may also be affected.

References:
http://www.debian.org/security/2005/dsa-763

- **avast! Antivirus ACE File Handling Two Vulnerabilities**
  "Execution of arbitrary code; Writing of files to arbitrary directories"

Secunia Research has discovered two vulnerabilities in avast!, which can be exploited by malicious people to compromise a vulnerable system.

1) An input validation error during extraction of ACE archives for scanning can be exploited to write files to arbitrary directories. This can be exploited when scanning a malicious archive containing a file that has the "/../" directory traversal sequence or an absolute path in its filename.

2) A boundary error in the scanning of ACE archives can be exploited to cause a stack-based buffer overflow when scanning a specially crafted ACE archive containing a file with a filename of more than 290 bytes.

Successful exploitation allows execution of arbitrary code and writing of files to arbitrary directories, but requires ACE archive scanning to be enabled.

The vulnerabilities have been confirmed in avast! Home/Professional Edition version 4.6.665 and Server Edition version 4.6.460. The vendor has reported that avast! Managed Client is also affected.

References:
http://secunia.com/secunia_research/2005-20/advisory/

- **Novell GroupWise WebAccess Script Insertion Vulnerability**

"Script insertion attacks"

Francisco Amato has reported a vulnerability in Novell GroupWise, which can be exploited by malicious people to conduct script insertion attacks.

Input passed in <IMG> HTML tags in emails is insufficiently sanitised in the WebAccess component before being displayed. This can be exploited to execute arbitrary script code in a user's browser session in context of a vulnerable site when a specially crafted email is displayed.

References:
http://support.novell.com/cgi-bin/search/searchtid.cgi?/10098301.htm
http://support.novell.com/cgi-bin/search/searchtid.cgi?/2971890.htm

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