netVigilance

ScoutNews Team **November 11, 2005**
Issue # 45

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

SONY's spyware backfires, IT brass say security top concern (echo) and DoD drops GSA.

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

- **SONY DRM woes grow**

"A thief believes everybody steals." - *Edward W. Howe*

SONY's new DRM software XCP, used on some of the company's music titles, prohibits Windows users from making more than three copies of any XCP-protected CD. The software, which SONY admits uses some of the same tactics as spyware or viruses to monitor user's activities.

Computer Associates is classifying Sony's software as spyware and its software will begin searching for and removing XCP with Sophos and possibly Kaspersky folling suit, Italy's cyber-crime investigation unit has been asked by the ALCEI-EFI (Association for Freedom in Electronic Interactive Communications - Electronic Frontiers Italy) to investigate the inclusion of the software as a cyber crime.

But wait, it gets worse; virus writers wasted no time in exploiting the XCP rootkit to spread a variant of the Breplibot Trojan. Systems with the SONY rootkit make the Trojan entirely invisible to the user.

Donna's Security Flash

Related Links :

http://www.macworld.co.uk/news/index.cfm?RSS&NewsID=13078

http://msmvps.com/donna/archive/2005/11/08/74851.aspx

http://www.theregister.co.uk/2005/11/10/sony_drm_trojan/

❖ IT Execs [still] nervous about network security

A recent survey done by AT&T in co-operation with the Economist Intelligence Unit (EIU); shows that network security is still the chief concern among IT executives, edging out cost, complexity and business disruption for 2nd, 3rd and 4th respectively.

IT executives see expanding electronic collaboration necessary to drive competitive advantages, but with more technology-based solutions come increased network vulnerability. Stan Quintana, Vice President, AT&T Managed Security Services put it this way: "The new capabilities of the ubiquitous network are great for commerce, but open a whole new dimension of risk."

Related Links:

http://www.indiainfoline.com/news/news.asp?dat=69411

http://www.lightreading.com/document.asp?doc_id=83935&WT.svl=wire1_1

❖ DoD takes IT procurements back from GSA

With the recent allegations of misallocation and misuse of funds to questionable fees and lack of administrative oversight; the GSA looses it's biggest customer, the Department of Defense (DoD).

Domenico Cippichio, deputy director for defense procurement for DoD stated that he would use GSA "when it makes the most sense."

VARBusiness

Full Story:

http://www.varbusiness.com/nl/government/showArticle.jhtml?sssdmh=dm4.157779&articleId=173600938

New Vulnerabilities Tested in SecureScout

❖ **12111** **Microsoft SQL Server Multiple Unchecked Buffer Vulnerabilities (ssnetlib.dll version check)**

Versions of Microsoft SQL Server 7 and Microsoft SQL Server 2000 contain various unchecked buffers which allow for a remote attacker to compromise the server in various ways, each with serious repercussions for the SQL Server.

Buffer overflow in SQL Server 7.0 and 2000 may allow a remote attacker to execute arbitrary code via a long OLE DB provider name to the OpenDataSource or OpenRowset in any normal connection.

Buffer overflows in extended stored procedures for Microsoft SQL Server 7.0 and 2000 may allow a remote attacker to cause a denial of service or execute arbitrary code via a database query with certain long arguments.

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

References:

@NO-MS02-020@
@NO-MS02-007@
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-020.asp
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-007.asp
http://www.securityfocus.com/bid/4231
http://www.securityfocus.com/bid/4135
SANS Top 20 Microsoft SQL Server (MSSQL): http://www.sans.org/top20/#W2

CVE Reference: CAN-2002-0056

❖ **12113** **Microsoft SQL Server Utilities Unchecked Buffer Vulnerability (ssnetlib.dll version check)**

Microsoft SQL Server 2000 has a buffer overflow vulnerability in several Database Consistency Checkers (DBCCs) and the Microsoft Desktop Engine (MSDE) 2000 that allows members of the db_owner and db_ddladmin roles to execute arbitrary code.

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

References:

@NO-MS02-038@
@NO-MS02-061@
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-038.asp

SANS Top 20 Microsoft SQL Server (MSSQL): http://www.sans.org/top20/#W2

CVE Reference: CAN-2002-0644, CAN-2002-0645

❖ 12114 Microsoft SQL Server Weak Permissions For Extended Stored Procedures Vulnerability (ssnetlib.dll version check)

Microsofts SQL Server / MSDE have a vulnerability which could allow unprivileged users, and possibly remote attackers, to run stored procedures with administrator privileges via xp_execresultset, xp_printstatements, or xp_displayparamstmt. Through use of these stored procedures a remote attacker may be able to execute arbitrary code on your machine.

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

References:

@NO-MS02-043@
@NO-MS02-061@
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-043.asp
SANS Top 20 Microsoft SQL Server (MSSQL): http://www.sans.org/top20/#W2

CVE Reference: CAN-2002-0721

❖ 13145 Microsoft SQL Server Hello Buffer Overflow Vulnerability (ssnetlib.dll version check)

SQL Server is a Microsoft database.
Some versions are vulnerable to a buffer overflow before the authentication occurs.
The buffer overflow occur in the first packet sent by the client to the server.
This allows any outsider to compromise your host

Test Case Impact: **Gather Info.** Vulnerability Impact: **High** Risk: **Gain root**

References:

@NO-MS02-061@
@NO-MS02-056@
CERT advisory: http://www.cert.org/advisories/CA-2002-22.html
BID: http://online.securityfocus.com/bid/5411
MS02-056:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-056.asp
Version 2 of MS02-061:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-061.asp
SANS Top 20 Microsoft SQL Server (MSSQL): http://www.sans.org/top20/#W2

CVE Reference: CAN-2002-1123

❖ **13309** **Oracle Database Server - Oracle Spatial component Unspecified error (oct-2005/DB18)**

An unspecified error in the Oracle Spatial component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

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

CVE Reference: CAN-2005-0873

❖ **13310** **Oracle Database Server - Oracle Spatial component Unspecified error (oct-2005/DB19)**

An unspecified error in the Oracle Spatial component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

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

CVE Reference: CAN-2005-0873

❖ **13311** **Oracle Database Server - Oracle Spatial component Unspecified error (oct-2005/DB20)**

An unspecified error in the Oracle Spatial component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

Product Homepage:

http://www.oracle.com/

CVE Reference: CAN-2005-0873

❖ 13312 Oracle Database Server - Oracle Spatial component Unspecified error (oct-2005/DB21)

An unspecified error in the Oracle Spatial component can potentially be exploited to disclose or manipulate information, to conduct PL/SQL injection attacks, cross-site scripting attacks.

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html

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

CVE Reference: CAN-2005-0873

❖ 14272 Microsoft SQL Server Multiple Buffer Overflows Vulnerability (ssnetlib.dll version check)

Microsoft SQL Server 2000 (MSDE version included) contains three flaws that result in a buffer overrun condition.
First one: Unchecked Buffer in Password Encryption Procedure that allows an attacker to to gain control of the database and execute arbitrary code via SQL Server Authentication;
Second one: Unchecked Buffer in Bulk Insert Procedure that allows attacker with database administration privileges to execute arbitrary code via a long filename in the BULK INSERT query;
Third one: Incorrect Permission on SQL Server Service Account Registry Key which allows local users to gain privileges.

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

References:

@NO-MS02-034@
@NO-MS02-061@
Microsoft Security Bulletin : http://www.microsoft.com/technet/security/bulletin/MS02-034.asp
SecurityFocus.com: http://online.securityfocus.com/bid/5205
http://online.securityfocus.com/bid/5014
http://online.securityfocus.com/bid/4847
Product Homepage: http://www.microsoft.com/sqlserver
SANS Top 20 Microsoft SQL Server (MSSQL): http://www.sans.org/top20/#W2
SANS Top 20 Windows Remote Access Services: http://www.sans.org/top20/#W5

CVE Reference: CAN-2002-0624, CAN-2002-0641, CVE-2002-0642

❖ **16031** **Vulnerabilities in Graphics Rendering Engine Could Allow Code Execution (MS05-053/896424) (Remote File Checking)**

A remote code execution vulnerability exists in the rendering of Windows Metafile (WMF) and Enhanced Metafile (EMF) image formats that could allow remote code execution on an affected system. Any program that renders WMF or EMF images on the affected systems could be vulnerable to this attack. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A remote code execution vulnerability exists in the rendering of Windows Metafile (WMF) image format that could allow remote code execution on an affected system. Any program that renders WMF images on the affected systems could be vulnerable to this attack. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A denial of service vulnerability exists in the rendering of Enhanced Metafile (EMF) image format that could allow any program that renders EMF images to be vulnerable to attack. An attacker who successfully exploited this vulnerability could cause the affected programs to stop responding.

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

References:

http://www.microsoft.com/technet/security/Bulletin/MS05-053.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2123
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2124
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0803

CVE Reference: CAN-2005-2123, CAN-2005-2124, CAN-2005-0803

New Vulnerabilities found this Week

SAP Web Application Server Multiple Vulnerabilities
"Cross-site scripting, phishing, and HTTP response splitting attacks."

Cybsec S.A. has reported some vulnerabilities in SAP Web Application Server, which can be exploited by malicious people to conduct cross-site scripting, phishing, and HTTP response splitting attacks.

1) Input passed to the "sap-syscmd" parameter in "fameset.htm" and the "BspApplication" field in the "SYSTEM PUBLIC" test application isn't properly sanitised before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

The vulnerabilities have been reported in versions 6.10, 6.20, 6.40, and 7.00, and affect the BSP runtime of SAP Web Application Server. Other versions may also be affected.

2) Input passed to the query string in pages generating error messages isn't properly sanitised before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

The vulnerability has been reported in version 6.10 and affects the BSP runtime of SAP Web Application Server. Prior versions may also be affected.

3) The problem is that an absolute URL for an external site can be specified in the "sapexiturl" parameter passed to "fameset.htm". This can be exploited to trick users into visiting a malicious web site by following a specially crafted link with a trusted hostname redirecting to the malicious web site.

The vulnerabilities have been reported in versions 6.10, 6.20, 6.40, and 7.00, and affect the BSP runtime of SAP Web Application Server. Other versions may also be affected.

4) Input passed to the "sap-exiturl" parameter isn't properly sanitised before being returned to the user. This can be exploited to inject arbitrary HTTP headers, which will be included in the response sent to the user.

The vulnerabilities have been reported in versions 6.10, 6.20, 6.40, and 7.00, and affect the BSP runtime of SAP Web Application Server. Other versions may also be affected.

References:
http://www.cybsec.com/vuln/CYBSEC_Security_Advisory_Multiple_XSS_in_SAP_WAS.pdf
http://www.cybsec.com/vuln/CYBSEC_Security_Advisory_Phishing_Vector_in_SAP_WAS.pdf
http://www.cybsec.com/vuln/CYBSEC_Security_Advisory_HTTP_Response_Splitting_in_SAP_WAS.pdf

SpamAssassin Long Message Header Denial of Service
“Denial of Service”

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

The vulnerability is caused due to the use of an inefficient regular expression in "/SpamAssassin/Message.pm" to parse email headers. This can cause perl to crash when it runs out of stack space and can be exploited via a malicious email that contains a large number of recipients.

The vulnerability has been reported in version 3.0.4. Prior versions may also be affected.

References:
http://issues.apache.org/SpamAssassin/show_bug.cgi?id=4570

Linux Kernel sysctl Interface Unregistration Denial of Service
“Denial of Service”

A vulnerability has been reported in the Linux kernel, 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 "sysctl.c" when handling the un-registration of interfaces in "/proc/sys/net/ipv4/conf/". This can potentially be exploited by malicious users to cause a DoS.

References:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.14.1
http://www.kernel.org/git/?p=linux/kernel/git/gregkh/linux-2.6.14.y.git;a=commit;h=e4e0411221c7d4f2bd82fa5e21745f927a1bff28

IBM Tivoli Directory Server Unspecified Security Bypass Vulnerability
"Change, modify and/or delete directory data"

A vulnerability has been reported in IBM Tivoli Directory Server (ITDS), which can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to an unspecified error and can be exploited to change, modify and/or delete directory data stored in the IBM Tivoli Directory Server.

The vulnerability has been reported in version 5.2.0 and 6.0.0.

ITDS is included with the following products:
* Tivoli Identity Manager version 4.6 (ITDS version 6.0.0).
* Tivoli Access Manager for Business Integration (AMBI) version 5.1 (ITDS version 5.2.0).
* Tivoli Access Manager for e-business (TAM) version 5.1 (ITDS version 5.2.0).
* Tivoli Access Manager for Operating Systems (TAMOS) version 5.1 (ITDS version 5.2.0).
* Tivoli Directory Integrator (ITDI) version 5.2 and version 6.0 (ITDS version 5.2.0).
* Tivoli Federated Identity Manager version 6.0 (ITDS version 5.2.0).
* Tivoli Intelligent ThinkDynamic Orchestrator, version 2.1.0 (ITDS version 5.2.0).
* Tivoli Intelligent Orchestrator, version 3.1.0 (ITDS version 5.2.0).
* Tivoli Provisioning Manager, version 2.1.0 (ITDS version 5.2.0).
* Tivoli Provisioning Manager, version 3.1.0 (ITDS version 5.2.0).
* WebSphere Business Integration for Healthcare Collaborative Network 1.0

References:
http://www-1.ibm.com/support/docview.wss?uid=swg21222172

Vulnerabilities in Graphics Rendering Engine Could Allow Code Execution
"Code Execution"

Vulnerabilities in Graphics Rendering Engine Could Allow Code Execution (896424)
A remote code execution vulnerability exists in the rendering of Windows Metafile (WMF) and Enhanced Metafile (EMF) image formats that could allow remote code execution on an affected system. Any program that renders WMF or EMF images on the affected systems could be vulnerable to this attack. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A remote code execution vulnerability exists in the rendering of Windows Metafile (WMF) image format that could allow remote code execution on an affected system. Any program that renders WMF images on the affected systems could be vulnerable to this attack. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A denial of service vulnerability exists in the rendering of Enhanced Metafile (EMF) image format that could allow any program that renders EMF images to be vulnerable to attack. An attacker who successfully exploited this vulnerability could cause the affected programs to stop responding.

References:
http://www.microsoft.com/technet/security/Bulletin/MS05-053.mspx

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