netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 32

August 11, 2006

Table of Contents

Product Focus

Sapphire Worm Scanner – The Sapphire Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Microsoft SQL buffer overflow vulnerability (MS02-039/MS02-061) that the recent Sapphire Worm uses to propagate.

This Week in Review

Microsoft invistes hackers to try and break Vista. ISSE conference on Security Management. Flaws in online systems passes even when known. How-to on hacking via Blackberry.

Enjoy reading & Stay safe

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

Top Security News Stories this Week

- **Microsoft to hackers: Take your best shot**

MS invites 3000 computer experts to hack Vista, the next generation of its Windows operating system
After suffering embarrassing security exploits over the past several years, Microsoft Corp. is trying a new tactic: inviting some of the world's best-known computer experts to try to poke holes in Vista, the next generation of its Windows operating system. Microsoft made

a test version of Vista available to about 3,000 security professionals Thursday as it detailed the steps it has taken to fortify the product against attacks that can compromise bank account numbers and other sensitive information.

Associated Press

Full Story :
http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?database=JanEE%2edb&command=viewone&id=99&op=t

❖ ISSE Brings Together Industry Authorities To Debate Technology, Legislation And Security Management

eema, the independent European association for e-business, today announced that Europe's largest debate on information security, Information Security Solutions Europe (ISSE) 2006, will be taking place in Rome from 10th-12th October. Split across four tracks, ISSE brings together technology users, governments, vendors, academics and legal professionals.

An extensive four-track programme compiled by TeleTrust comprising Technology; Legal, Data Protection & Compliance; Security Management; Trusted Computing; as well as Italian and German workshops, will cover the three days. Each track will deal with the hottest security topics today including Identity Management, e-Identification, PKI, Biometrics, Technical Solutions, Trusted Computing, Emerging Security Technologies, Security Management, Privacy & Data Protection, Cyberspace Regulations, Security Measurements, Security standards, Awareness Raising, e-Government Applications, e-Health Applications and European IT Security Projects.

The IT Shield

Full Story :
http://www.theitshield.com/pr/9445

❖ HSBC knew about security loophole in online banking

One of Britain's biggest high street banks knew about a security loophole in its online banking service that left millions of accounts open to fraud and did nothing about it for almost two years. HSBC initially denied the defect in its computer banking but conceded yesterday that the problem had been known about since the system was introduced.

The defect, uncovered by researchers at Cardiff University and exposed in yesterday's Guardian, was the result of a conscious decision by those building the system two years ago, a spokesman for the bank said. "It wasn't there accidentally," he said. "When the system was being designed, research was done into it and the decision was made [to leave the loophole]. Often times these are judgment calls."

The Guardian

Full Story :
http://technology.guardian.co.uk/news/story/0,,1842177,00.html

❖ BlackBerry hacking peril exposed

Blackjacking circumvents corporate defences
A hacking program, due to be released next week, will demonstrate how to use a connection from BlackBerry devices to potentially bypass enterprise security defences.

Jesse D'Aguanno, director of security research at German firm Praetorian Global, gave a presentation on how to use the BlackBerry environment to circumvent perimeter defenses and directly attack hosts on a corporate intranet at last week's DefCon conference in Vegas. The demo included a live presentation. Next week D'Aguanno plans to release source code for BBProxy, the tool used to conduct the attack, which he describes as "Blackjacking".

The Register

Full Story :
http://www.theregister.co.uk/2006/08/10/blackjack_hack_attack/

New Vulnerabilities Tested in SecureScout

- **13398 Oracle Database Server - Username buffer overflow**

During the authentication process of connecting to an Oracle database, a username and password are sent to the server. Typically client applications, particularly those from Oracle, are designed to limit the length of the username passed in for authentication. However, if a username of 1150 characters or greater is passed to the authentication mechanism, a buffer overflow occurs. This overflow occurs before authentication occurs, so an unauthenticated attacker could use this buffer overflow to gain full control of a database.

This buffer overflow does not result in the Oracle process crashing. However the buffer overflow does result in the saved return address being overwritten on the stack.

Although most applications truncate the username, one program included in the Oracle utilities is known to allow long usernames. The loadpsp utility found in the $ORACLE_HOME/bin directory can be called as follows:

C:\oracle\bin> loadpsp -name -user XXX[1150 additional characters]/test@iasdb test

The issue is fixed in the 9.2.0.3, 9.0.1.5, 8.1.7.5

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

References:

Original Advisory:
http://otn.oracle.com/deploy/security/pdf/2003alert51.pdf

Other references:
https://www.appsecinc.com/Policy/PolicyCheck62.html

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

CVE Reference: CVE-2003-0005

❖ 13399 Oracle Database Server - TZ_OFFSET buffer overflow

Oracle database provides a built-in function called TZ_OFFSET which returns the time zone offset corresponding to the value entered based on the date the statement is executed. You can enter a valid time zone name, a time zone offset from UTC (which simply returns itself), or the keyword SESSIONTIMEZONE or DBTIMEZONE.

A buffer overflow exists in the TZ_OFFSET function. This buffer overflow occurs when a long string is passed as the second parameter of the function. Below is an example:

SELECT TZ_OFFSET('US/EasternXXXX[74 additional Xs]') FROM DUAL;

The buffer overflow occurs as the database attempts to copy the time zone name into a buffer on the stack. This buffer overflow does not result in the Oracle process crashing. However the buffer overflow does result in the saved return address being overwritten on the stack.

A user needs no privileges to execute this function. This security issue allows a non-privileged user to elevate his or her privileges to DBA.

The issue is fixed in the 9.2.0.3, 9.0.1.5, 8.1.7.5

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/2003alert50.pdf

Other references:
https://www.appsecinc.com/Policy/PolicyCheck64.html

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

CVE Reference: CVE-2003-0005

❖ 13400 Oracle Database Server - BFILENAME buffer overflow

The Oracle database provides a built-in function called BFILENAME. BFILENAME is used to return a BFILE locator which is associated with a physical LOB binary file. The function accepts two parameters: DIRECTORY and FILENAME.

The buffer overflow occurs as Oracle attempts to copy the DIRECTORY value into a buffer on the stack. This buffer overflow does not result in the Oracle process crashing. However the buffer overflow does result in the saved return address being overwritten on the stack.

A user needs no privileges to execute this function. This security issue allows a non-privileged user to elevate his or her privileges to DBA.

The issue is fixed in the 9.2.0.3, 9.0.1.5, 8.1.7.5

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/2003alert48.pdf

Other references:
https://www.appsecinc.com/Policy/PolicyCheck65.html

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

CVE Reference: CVE-2003-0005

❖ 13401 Oracle Database Server - Database link buffer overflow

A database link is a mechanism within an Oracle database to provide location transparency to read data from other databases. It is essentially a pointer to another database. The pointer is an entry in the data dictionary which includes the name of the remote server, a connection string, and possibly a username and password to authenticate to the remote system.

A database link is created using the following syntax:

CREATE DATABASE LINK [linkname] CONNECT TO [username] IDENTIFIED BY [password] USING '[connection string]'

If you designate a connection string longer than 1000 characters, the long value is saved into the data dictionary. The buffer overflow does not actually occur in this function. It is later when the database link is accessed that the buffer overflow occurs. The following command will cause the buffer overflow:

SELECT * FROM TEST@[linkname]

This buffer overflow does not result in the Oracle process crashing. However the buffer overflow does result in the saved return address being overwritten on the stack.

A user must have the CREATE DATABASE LINK privilege in order to execute this attack. By default the CONNECT role is granted this privilege, so an account such as SCOTT with a password of TIGER would allow any attacker to connect to the system, create a database link, and then select the database link.

The issue is fixed in the 9.2.0.3, 9.0.1.5, 8.1.7.5

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/2003alert54.pdf

Other references:
https://www.appsecinc.com/Policy/PolicyCheck66.html

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

CVE Reference:

❖ 13402 Oracle Database Server - EXTPROC buffer overflow

The EXTPROC (external procedure) service in Oracle allows a PL/SQL packages to load and call functions in operating system libraries or dynamic link libraries (DLLs). Whenever a call to load a function in an external library is made, the Oracle process contacts the Listener process. The Listener process in turn connects to the EXTPROC service and passes the name of the library and the requested function to it. There is absolutely no authentication involved in this process.

An attacker can pretend to be the Oracle service and request the Listener process to call functions in the external operating system libraries. Since there is no authentication the Listener will accept the call and run the EXTPROC utility, which in turn will call the actual function in the library.

The functionality in Oracle was changed in version 9.2.0.1.0 to prevent this by only allowing calls to the libraries available in $ORACLE_HOME\bin directory. As well, the EXTPROC still allows connections over TCP/IP but doesn't service any remote calls. All these failed calls to EXTPROC get logged to a log file. There exists a buffer overflow with this logging functionality of EXTPROC. If the remote user tries to load a library with an overly long name, the EXTPROC rejects it and tries to log the library name. It's during this process that the saved return address gets overwritten on the stack, allowing a malicious remote user to execute code of his choice.

Even if the EXTPROC limits the libraries that can be loaded to only the $ORACLE_HOME\bin directory, there are several hundred shared libraries in that directory, many of which may contain buffer overflows.

The issue is fixed in the 9.2.0.4

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/2003alert57.pdf

Other references:
https://www.appsecinc.com/Policy/PolicyCheck68.html

Product Homepage:

http://www.oracle.com/

CVE Reference:

❖ 13403 Oracle Database Server - XDB HTTP username buffer overflow

Oracle XML Database (XDB) is a set of built-in high-performance storage and retrieval technologies developed especially for XML.

The Oracle XDB can be accessed via its HTTP service. The service runs on port 8080 and is enabled by default. Users need to be authenticated in order to use this service.

There exists a buffer overflow vulnerability with the way username and passwords are handled by this service.

A malicious attacker can cause the stack based buffer to overflow by supplying it with an overly long username or password during the process of authentication. This can lead to full remote system compromise and / or Denial of Service (DoS).

The issue is fixed in the 9.2.0.4

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/2003Alert58.pdf

Other references:
https://www.appsecinc.com/Policy/PolicyCheck69.html

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

CVE Reference:

❖ 13404 Oracle Database Server - XDB FTP TEST buffer overflow

Oracle XML Database (XDB) is a set of built-in high-performance storage and retrieval technologies developed especially for XML.

The Oracle XDB can be accessed via its FTP service. The service runs on port 2100 and is enabled by default. Users need to be authenticated in order to issue any FTP service commands.

Along with other FTP commands, this service supports the TEST command. There exists a buffer overflow vulnerability with the way parameters are handled by this command.

A malicious attacker can cause the buffer to overflow by supplying it with an overly

long parameter. This allows the hacker to run arbitrary commands under the privileges of the XDB FTP service.

The issue is fixed in the 9.2.0.4

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/2003Alert58.pdf

Other references:
https://www.appsecinc.com/Policy/PolicyCheck71.html

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

CVE Reference:

❖ 13405 Oracle Database Server - SSL vulnerabilities

Secure Sockets Layer (SSL) is an industry standard protocol used to communicate securely over a network. A series of vulnerabilities exist in the SSL libraries used by the Oracle database. Oracle uses the OpenSSL libraries (www.openssl.org) in its implementation of network encryption. These vulnerabilities result in several security concerns, ranging from information (including key) leakage to full exploitation of the system running the SSL libraries.

The vulnerabilities relate to the ASN.1 parsing the SSL libraries perform when handling X.509 certificates. For full details on the vulnerabilities, reference the CERT advisory at http://www.cert.org/advisories/CA-2003-26.html.

The Oracle database server uses these libraries and as such is vulnerable to these security risks.

The issue is fixed in the 9.2.0.5, 9.0.1.5, 8.1.7.5

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

References:

Original Advisory:
http://www.openssl.org/news/secadv_20030930.txt
http://www.cert.org/advisories/CA-2003-26.html

Other references:
https://www.appsecinc.com/Policy/PolicyCheck75.html

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

CVE Reference:

❖ 13406 Oracle Database Server - NUMTODSINTERVAL buffer overflow

The NUMTODSINTERVAL function converts a number to an INTERVAL DAY TO SECOND literal. The syntax for the numtodsinterval function is "numtodsinterval (number, expression)" where number is the number to convert to an interval and expression is the unit. Expression must be one of the following values: DAY, HOUR, MINUTE, SECOND.

A buffer overflow exists in the NUMTODSINTERVAL function. This buffer overflow occurs when a long string is passed as the second parameter of the function. Below is an example:

select NUMTODSINTERVAL(100000000, 'XXXX[1000+]') from dual;

The buffer overflow occurs as the database attempts to parse the format string passed as the second parameter. The buffer overflow results in the saved return address being overwritten on the stack.

A user needs no privileges to execute this function. This security issue allows a non-privileged user to elevate his or her privileges to DBA.

The issue is fixed in the 9.2.0.5, 9.0.1.5

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/2004alert64.pdf

Other references:
https://www.appsecinc.com/Policy/PolicyCheck82.html

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

CVE Reference:

❖ 13407 Oracle Database Server - DBMS_REPCAT sname oname overflow

The Oracle database provides a set of packages that can be used to administer a replicated environment. Some procedures of these packages use the parameters "sname" to specify a schema name and "oname" to specify an object name. When a long string is passed to this parameter a buffer overflow occurs.

Below are some examples that exploit this vulnerability.

```
BEGIN
DBMS_REPCAT.ADD_GROUPED_COLUMN ('longstring', 'longstring', 'cc', 'dd');
END;
```

or

```
BEGIN
DBMS_REPCAT.ADD_DELETE_RESOLUTION ('longstring', 'longstring', 0, ",");
END;
```

or

```
BEGIN
DBMS_REPCAT.CANCEL_STATISTICS ('longstring', 'longstring');
END;
```

This vulnerability can be exploited by members of the roles EXECUTE_CATALOG_ROLE and SYSDBA or by users granted execute permissions on these vulnerable packages.

This security issue allows a non-privileged user to elevate his or her privileges to DBA. It can also be exploited to crash the database causing a DOS (Denial of Service) condition for the Oracle database.

The issue is fixed in the 9.2.0.5

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

References:

Original Advisory:
http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf

Other references:
https://www.appsecinc.com/Policy/PolicyCheck88.html

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

CVE Reference:

New Vulnerabilities found this Week

Sun Solaris "drain_squeue()" Denial of Service

"Denial of Service"

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

The vulnerability is caused due to an unspecified error, which can be exploited to cause system panics in the "drain_squeue()" function during a high load of TCP connections.

NOTE: It is reportedly unlikely that this affects systems not using CMT processors.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102554-1

Microsoft Windows Two Vulnerabilities

"Gain escalated privileges"

Two vulnerabilities have been reported in Microsoft Windows, which can be exploited by malicious, local users to gain escalated privileges and by malicious people to compromise a vulnerable system.

1) An error in Winlogon when searching for DLL files when applications are started can be exploited by a malicious, local user to gain escalated privileges by placing a malicious DLL file in the user directory.

NOTE: Only Windows 2000 is affected by default as other OS versions have "SafeDllSearchMode" set to "1" by default.

2) An error in the exception handling management when multiple applications are resident in memory can be exploited to execute arbitrary code by tricking a user into visiting a malicious website.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-051.mspx

Microsoft Visual Basic for Applications Buffer Overflow
"Execution of arbitrary code"

A vulnerability has been reported in Microsoft Visual Basic for Applications, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the way document properties are passed from a host application when opening a document and can be exploited to cause a buffer overflow.

Successful exploitation allows execution of arbitrary code when a user e.g. opens a specially crafted Office document or visits a malicious website.

NOTE: According to the vendor, the vulnerability is being actively exploited in the wild.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-047.mspx

Windows Kernel Privilege Escalation Vulnerability
"Gain escalated privileges"

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

The vulnerability is caused due to an unspecified boundary error in the kernel and can be exploited to cause a buffer overflow.

Successful exploitation allows execution of arbitrary code with kernel-level privileges.

NOTE: Additional issues discovered internally by Microsoft have also been reported.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-049.mspx

PHP "sscanf()" Code Execution Safe Mode Bypass

"Bypass of the safe mode"

Heintz has discovered a vulnerability in PHP, which potentially can be exploited by malicious, local users to bypass certain security restrictions.

The vulnerability is caused due to an array boundary error in the "sscanf()" PHP function in the processing of the "$1s" format specifier. This can be exploited to reference freed memory by passing a variable as argument which has been unset.

Successful exploitation may e.g. allow bypass of the safe mode protection by executing arbitrary code.

The vulnerability has been confirmed in versions 5.1.4 and 4.4.3. Other versions may also be affected.

References:
http://bugs.php.net/bug.php?id=38322

Microsoft Management Console Cross-Site Scripting

"Cross-site scripting attacks"

A vulnerability has been reported in Microsoft Windows, which can be exploited by malicious people to conduct cross-site scripting attacks.

The vulnerability is caused due to an input validation error in the Microsoft Management Console (MMC) as HTML embedded resource files in the MMC library can be directly referenced from the Internet or Intranet zones via Internet Explorer.

Successful exploitation allows execution of arbitrary script code in context of the "My Computer" zone.

NOTE: Internet Explorer 5.01 users are vulnerable from URLs in the "Internet" Zone. Internet Explorer 6 SP1 users are by default only vulnerable from URLs in the "Intranet" Zone as access to local files is blocked.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-044.mspx

Internet Explorer Multiple Vulnerabilities

"Gain knowledge of certain information; compromise a user's system"

Multiple vulnerabilities have been reported in Internet Explorer, which can be exploited by malicious people to gain knowledge of certain information or compromise a user's system.

1) An error in the interpretation of HTML with certain layout positioning combinations can be exploited to corrupt memory and execute arbitrary code via a specially crafted web page.

2) An error in the way chained Cascading Style Sheets (CSS) are handled can be

exploited to corrupt memory and execute arbitrary code via a specially crafted web page.

3) Another error in the HTML rendering can be exploited to corrupt memory and execute arbitrary code via a specially crafted web page.

4) An error exists in the "TupleNthBvrImpl::GetTypeInfo()" function in the DirectAnimation.DATuple ActiveX control (danim.dll) when instantiating it in Internet Explorer. This can be exploited to execute arbitrary code by supplying a specially crafted, positive integer to the "Nth()" method.

5) Other errors in the way Internet Explorer instantiates COM objects not intended to be instantiated in the browser can be exploited to execute arbitrary code via a specially crafted web page.

6) An error in the way the origin of a script is determined can be exploited to run a script in another domain or security zone than intended via a specially crafted web page.

7) Script may persist across navigations making it possible to use the script to access the window location of a web page in another domain or security zone.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-042.mspx

Windows DNS Resolution Code Execution Vulnerabilities
"Execution of arbitrary code"

Some vulnerabilities have been reported in Microsoft Windows, which can be exploited by malicious people to compromise a vulnerable system.

1) A boundary error in the Winsock API when handling hostnames can be exploited to cause a buffer overflow by either tricking a user into opening a file or visiting a specially crafted website.

Successful exploitation allows execution of arbitrary code.

2) Some errors exist in the DNS Client service when processing DNS responses. This can be exploited to corrupt memory by returning a DNS response with a specially crafted "TXT", "HINFO", "X25", "ISDN", or "ATMA" record.

Successful exploitation allows execution of arbitrary code.

References:
http://www.microsoft.com/technet/security/Bulletin/MS06-041.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