netVigilance

ScoutNews Team

1 October 2004
Issue #40

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Just as Alan Wade from CIA endorses IM being a powerful application we see an active worm spreading through AIM.

Windows SP2 for XP is proving to be trickier than usual service packs. Most corporations have not deployed the patch as of now and the individual users that have done so are having problems with the fact.

Enjoy reading

Top Security News Stories this Week

❖ Spies work on info sharing

Officials in the intelligence community have started several initiatives related to information technology tagging, collaboration and acquisition to improve data-sharing among personnel of all security levels.
They believe data can be published after information about how it was acquired is removed. "It's all about the data," said Alan Wade, chief information officer for the CIA. He spoke Sept. 29 at the Government Symposium on ISR Transformation.

http://www.fcw.com/fcw/articles/2004/0927/web-info-09-30-04.asp
Frank Tiboni

❖ Windows JPEG worm spreading over AOL IM

IM messages direct users to websites with infected images…
A worm that exploits the recently discovered JPEG vulnerability has been discovered spreading over AOL's Instant Messenger (IM).
"It's been done in the past, but with HTML code instead of the JPEG," said Johannes Ullrich, CTO for SANS' Internet Storm Center, the organisation's online security research unit. "It is a virus, but it didn’t spread very far. We've only had two reports of it."
http://software.silicon.com/malware/0,3800003100,39124582,00.htm
Dan Ilett

❖ New Windows Patch Proves Tricky

The emergence of a new Internet virus targeting a Microsoft Windows security flaw could cause more damage than usual because the company's system for fixing the problem is so complex that many people will not bother to download it, security experts warned.

On Sept. 14, Microsoft released a patch to remedy a problem in the way the company's products process digital image files. That problem could allow attackers to take control of computers running the Windows XP (news - web sites) operating system, Server 2003 software and Microsoft Office just by getting people to open an e-mail message or visit a Web site. Microsoft Office is a bundle of products that includes the popular Word, Excel and Outlook e-mail programs.

http://story.news.yahoo.com/news?tmpl=story&cid=1804&e=2&u=/washpost/20041001/tc_washpost/a64737_2004oct1

Brian Krebs

New Vulnerabilities Tested in SecureScout

❖ 12109 Oracle9i Application Server Web Cache Heap-based buffer overflow Vulnerability

Security vulnerabilities have been discovered in Oracle Application Server Web Cache 10g (9.0.4.0.0) and Oracle9i Application Server Web Cache.

By default Web Cache listens for incoming connections on port 7777 for HTTP and 4443 for HTTPS.

A heap overflow condition exists in "webcached" process when an invalid HTTP/HTTPS request is made.

The overflow can be triggered by sending an overly long header as the HTTP Request Method.

Based on the version of your current Oracle Server, your Application Server Web Cache component is vulnerable.

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

CVE Links: CAN-2004-0385

Reference: http://www.inaccessnetworks.com/ian/services/secadv01.txt & http://otn.oracle.com/deploy/security/pdf/2004alert66.pdf & http://www.oracle.com/

❖ 13015 Oracle E-Business Suite Multiple Non-descript SQL Injection Vulnerability

Oracle E-Business Suite and Oracle Applications contain several flaws that will allow an attacker to inject arbitrary SQL code. These vulnerabilities can be remotely exploited by using a browser to send a specially crafted URL to the web server. No further details are available.

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

CVE Links: CAN-2004-0543

Reference: http://www.integrigy.com/alerts/OraAppsSQLInjection.htm & http://otn.oracle.com/deploy/security/pdf/2004alert67.pdf & http://www.oracle.com/

❖ 13174 Oracle Database Server dbms_system.ksdwrt Buffer Overflow

Vulnerability

Remote exploitation of a buffer overflow vulnerability in Oracle Corp.'s Oracle Database Server could allow attackers to crash the server and potentially execute arbitrary code. The problem specifically exists within dbms_system.ksdwrt(), a function that allows writing messages to alert.log. If a long string is passed as the second argument to this function, a buffer overflow occurs.

Successful exploitation allows authorized remote users to cause the Oracle server process to crash and potentially execute arbitrary code.

Authorized users include any users who are members of the SYS or SYSTEM roles, as well as users who are granted execute permissions on the dbms_system package.

Successful exploitation of this vulnerability on Microsoft Corp.'s Windows platforms can lead to a full system compromise, as most systems are configured to run the Oracle service under Local System. Successful exploitation of this vulnerability on Linux/Unix platforms usually compromises only the database because the Oracle service runs under a non-privileged account.

In cases where Oracle Internet Directory has been installed, an added exploitation vector exists. This is because Oracle Internet Directory creates a database user called ODSCOMMON that has a default password of ODSCOMMON which cannot be changed, thereby allowing any attacker to connect to the database server and exploit this vulnerability.

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

CVE Links: CAN-2004-0638

Reference:
http://www.idefense.com/application/poi/display?id=135&type=vulnerabilities&flashstatus=true & http://otn.oracle.com/deploy/security/pdf/2004alert68.pdf & http://www.oracle.com/

❖ 13204 RealOne Player / RealPlayer / Helix Player Multiple Vulnerabilities (Remote File Checking)

RealNetworks Inc. has recently been made aware of security vulnerabilities that could potentially allow an attacker to run arbitrary or malicious code on a user's machine. While we have not received reports of anyone actually being attacked with this exploit, all security vulnerabilities are taken very seriously by RealNetworks Inc. Real has found and fixed the problem.

The specific exploits were:

* Exploit 1: To fashion an RM file which corrupts the Player when run from a local drive and which might allow an attacker to execute arbitrary code on a user's machine.
* Exploit 2: To fashion a web page with malformed calls, corrupting the embedded Player, and which might allow an attacker to execute arbitrary code on a user's machine.
* Exploit 3: To fashion a web page and a media file to allow deletion of a file in a path known to the attacker.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://service.real.com/realplayer/security/ &
http://www.service.real.com/help/faq/security/040928_player/EN/

- **13205 Oracle Database Server ctxsys.driload Access Validation Vulnerability**

  Remote exploitation of an access validation vulnerability in multiple versions of Oracle Corp.'s Oracle Database Server could allow authenticated users to obtain administrative privileges.

  The problem specifically exists because although Oracle 9i Databases have the account ctxsys locked by default, ctxsys.driload is still accessible by users. The package ctxsys.driload allows every user to execute commands as DBA. A database connection with execute permissions on the package ctxsys.driload is required.

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

CVE Link: CAN-2004-0637

Reference:
http://www.idefense.com/application/poi/display?id=136&type=vulnerabilities&flashstatus=true & http://otn.oracle.com/deploy/security/pdf/2004alert68.pdf & http://www.oracle.com/

- 14044 **RealOne Player / RealPlayer Multiple Vulnerabilities (Remote File Checking)**

  RealNetworks Inc. has recently been made aware of security vulnerabilities that could potentially allow an attacker to run arbitrary code on a user's machine. While we have not received reports of anyone actually being attacked with this exploit, all security vulnerabilities are taken very seriously by RealNetworks Inc. Real has found and fixed the problem.

  The specific exploits were:

  * To fashion RAM files which corrupt the Player and which might allow an attacker to execute arbitrary code on a user's machine. Multiple issues were reported in this area.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://service.real.com/realplayer/security/ &
http://service.real.com/help/faq/security/040610_player/EN/

- **14109 RealPlayer / RealOne Player / ReaPlayer Enterprise Multiple Vulnerabilities (Remote File Checking)**

  RealNetworks Inc. has recently been made aware of a security vulnerability that could potentially allow an attacker to run arbitrary code on a user's machine.
  The specific exploit was:
  * To fashion an R3T media file to create a “Buffer Overrun” error.
  While we have not received reports of anyone actually being attacked with this exploit and though the percentage of players with this plug-in is very small, all security vulnerabilities are taken very seriously by RealNetworks Inc. Real has found and fixed the problem.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://service.real.com/help/faq/security/040406_r3t/en/ &
http://service.real.com/realplayer/security/

❖ 14143 RealOne Player / RealPlayer / RealOne Enterprise / RealPlayer Enterprise Multiple Vulnerabilities (Remote File Checking)

RealNetworks, Inc. has recently been made aware of security vulnerabilities that could potentially allow an attacker to run arbitrary code on a user's machine.
The specific exploits were:
* Exploit 1: To operate remote Javascript from the domain of the URL opened by a SMIL file or other file.
* Exploit 2: To fashion RMP files which allow an attacker to download and execute arbitrary code on a user's machine.
* Exploit 3: To fashion media files to create “Buffer Overrun” errors.
While we have not received reports of anyone actually being attacked with this exploit, all security vulnerabilities are taken very seriously by RealNetworks. RealNetworks has found and fixed the problem.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://service.real.com/help/faq/security/040123_player/EN/ &
http://service.real.com/realplayer/security/

❖ 14158 RealOne Player / RealOne Enterprise Desktop / RealOne Player Multiple Vulnerabilities (Remote File Checking)

The specific exploits were:
* Exploit 1: To embed scripts and/or false URLs in temporary files written by the Player before being executed by the default Web browser.
* Exploit 2: To operate remote Javascript or VBScript from the domain of the URL opened by a SMIL or other file.
While we have not received reports of anyone actually being attacked with this exploit, all security vulnerabilities are taken very seriously by RealNetworks. RealNetworks has found and fixed the problem.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://service.real.com/realplayer/security/ &
http://service.real.com/help/faq/security/securityupdate_october2003.html

❖ 15132 Winamp Fasttracker 2 Plug-In in_mod.dll Overflow Vulnerability (Remote File Checking)

The Winamp Player is a flexible and sophisticated application for playing and managing music.

An overflow exists in Nullsoft WinAmp. WinAmp fails to perform a proper boundary check within the in_mod.dll plugin when loading Fasktrackker 2 (".xm") media files resulting in a heap-based buffer overflow. With a specially crafted request, an attacker can cause execution of arbitrary code resulting in a loss of integrity.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.nextgenss.com/advisories/winampheap.txt & http://www.winamp.com/ & http://www.securityfocus.com/bid/10045

New Vulnerabilities found this Week

- **Illustrate dBpowerAMP Music Converter and Audio Player Buffer Overflow Vulnerabilities**

"Remote buffer overflow"

dBpowerAMP Music Converter and Audio Player reported prone to remote buffer overflow vulnerabilities when processing malformed audio and playlist files. This issue exists due to insufficient boundary checks performed by the applications and may allow an attacker to gain unauthorized access to a vulnerable computer.

Reportedly, these issues affect dBPowerAmp Music Converter 10.0 and Audio Player 2.0. Other versions may be vulnerable as well.

References:
http://www.dbpoweramp.com/
http://www.securityfocus.com/bid/11266

- **Microsoft SQL Server Remote Denial Of Service Vulnerability**

"Remote denial of service"

Reportedly Microsoft SQL Server is affected by a remote denial of service vulnerability. This issue is due to a failure of the application to handle irregular network communications.

An attacker may leverage this issue to cause the affected server to crash, denying service to legitimate users.

References:
http://www.microsoft.com/sql/default.asp
http://www.securityfocus.com/archive/1/376929

- **BroadBoard Message Board Multiple SQL Injection Vulnerabilities**

"SQL injection vulnerabilities "

Reportedly BroadBoard Message Board is affected by multiple SQL injection vulnerabilities. These issues are due to a failure of the application to properly sanitize user supplied URI input prior to using it in an SQL query.

An attacker may exploit these issues to manipulate SQL queries, potentially revealing or corrupting sensitive database data. These issues may also facilitate attacks against the underlying database software.

References:
http://www.securityfocus.com/bid/11250/

- **YahooPOPS! Multiple Remote Buffer Overflow Vulnerabilities**

“Buffer overflow vulnerabilities:”

It is reported that YahooPOPS! contains multiple buffer overflow vulnerabilities. These vulnerabilities are due to a failure of the application to properly bounds check user-supplied input data before copying it into finite sized memory buffers. This allows attackers to overwrite adjacent memory, potentially overwriting critical memory structures and altering the flow of execution. This will likely allow for remote code execution in the context of the affected application.

Versions of YahooPOPS! from 0.4 through to, and including 0.6 are reportedly affected by these vulnerabilities.

References:
http://yahoopops.sourceforge.net/

- **Symantec Norton AntiVirus Malformed EMail Denial Of Service Vulnerability**

“Denial of service vulnerability”

It is alleged that Symantec Norton AntiVirus is prone to a denial of service vulnerability.

The discoverer of this issue reports that when a malformed email is received through Microsoft Outlook and Norton AntiVirus attempts to process this email, the Norton AntiVirus application will crash.

Symantec is currently investigating this report; this BID will be updated as soon as this investigation is complete. It should also be noted that the discoverer of the issue has not provided any details about which versions may be affected by this issue, version information will be updated appropriately when this issue is investigated further.

References:
http://www.securityfocus.com/archive/82/376487/2004-09-24/2004-09-30/0

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