ScoutNews Team **8 October 2004**
Issue #41

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Lots of news this week!
As video over IP starts to get deployed with more and more high value applications the JPEG protocol is compromised – this is an important area to get patched.
Disaster readiness is improving, however not at the rate it should be. One can ask the question: "Are we just living with an unacceptable level of insecurity?"
T-mobile is tightening its hotspot security by implementing WEP, this will make it a bit harder for the hackers to steal identities, but not impossible.

Enjoy reading

Top Security News Stories this Week

- **Security Firm Finds Program to Create JPEGs Exploiting Microsoft Flaw**

Panda Software reported finding a tool on black hat hacker sites that can be used to create files in the JPEG image format that exploit the vulnerability in Microsoft's JPEG processing component.
Microsoft patched the flaw on Sept. 14 in security bulletin MS04-028, but because the flaw affects so many products and the patch must be applied to each of the applications on every system, it is a difficult patch to apply.

http://entmag.com/news/rss.asp?editorialsid=6396
Scott Bekker

- **Study Questions Disaster Readyness**

A national survey released on Tuesday revealed a considerable discrepancy between perception and reality concerning the disaster preparation of Fortune 1000 companies, according to C-suite executives. The study, commissioned by SunGard Availability Services (availability.sungard.com) and conducted by Harris Interactive (harrisinteractive.com), discovered potential deficiencies in companies' ability to access critical information when faced with power outages, natural disasters, hackers and computer viruses.
http://thewhir.com/marketwatch/stu100704.cfm

- **T-Mobile boosts public WLAN security**
  T-Mobile has begun using 802.1x security to authenticate users logging on to its US pubic Wi-Fi hotspots in a bid to make it harder for hackers to obtain legitimate users' names and passwords.
  The move replaces the company's traditional web-based login system with an updated version of its own utility, Connection Manager, or software built into Windows XP and Mac OS X.
  Not only is the initial login more secure, but users' connections will now be encrypted.
  Traditional, web-based gateways control between the open WLAN and the Internet. This method was favoured because it didn't require the user to walk through a complex set-up process at each hotspot in order to ensure a secure connection. Even then, 802.11's Wired Equivalent Protection (WEP) security system is not the most robust of security standards.

http://www.theregister.co.uk/2004/10/06/t-mobile_wifi_security/
Tony Smith

New Vulnerabilities Tested in SecureScout

- **13175 Skype Installed (Remote File Checking)**
  Skype is a free program that uses the latest P2P (cutting edge p2p technology) technology to bring affordable and high-quality voice communications to people all over the world. Skype may not be suitable for a business environment.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://www.skype.com/

- **14163 RealOne Player / RealOne Enterprise Desktop Multiple Vulnerabilities (Remote File Checking)**
  The specific exploit was: To operate remote Javascript or VBScript from the domain of the URL opened by a SMIL file.

  Note: A small number of presentations may be disabled by this fix, for instance those that call javascript as an embedded event in an .RM file. In the stated example, it is recommended to move all javascript to a page that is opened with an embedded event via an http call. For further information or suggestions please refer to the RealNetworks Support Area which includes areas for documentation, community support and code samples.
  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 Links: GENERIC-MAP-NOMATCH

Reference: http://service.real.com/realplayer/security/ &
http://service.real.com/help/faq/security/securityupdate_august2003.html

- **14275 RealOne Player / RealPlayer / RealOne Enterprise Desktop Manager and RealOne Enterprise Desktop Multiple Vulnerabilities (Remote File Checking)**
  By creating a specifically corrupted PNG (Portable Network Graphics) file, it is possible to cause heap corruption to occur, allowing an attacker to execute 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. RealNetworks has found and fixed the problem.
  This vulnerability was due to the usage of an older, vulnerable version of a data-compression library within the RealPix component of the Player. The vulnerability was fixed by using an updated (non-vulnerable) version of this data-compression library in RealPix.
  In addition to fixing the reported vulnerability, RealNetworks performed a review of all of the RealOne Player source code to identify other areas where this data-compression library is used. As a result of this review, several additional Player components have also been fixed, and are included in the provided updates.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://service.real.com/realplayer/security/ &
http://service.real.com/help/faq/security/securityupdate_march2003.html

- **14470 RealOne Player / RealOne Player / RealOne Enterprise Desktop Manager / RealOne Enterprise Desktop Multiple Vulnerabilities (Remote File Checking)**
  Please use the links below to update your Player to one that includes the identified fixes.

  While we have not received reports of anyone actually being attacked with this exploit, all security vulnerabilities are taken very seriously by RealNetworks. In addition to fixing reported vulnerabilities, RealNetworks performed a comprehensive review of all of the RealOne Player source code to reduce the chance that any vulnerabilities remain.

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/bufferoverrun_update.html

- **14659 RealOne Player Gold / RealJukebox2 / RealJukebox 2 Plus Multiple Vulnerabilities (Remote File Checking)**
  1. Commonly known as a "buffer overrun", this could allow an attacker to run arbitrary code on a user's machine.
  2. This exploit could allow an attacker to load an HTML page in the My Computer security domain and execute code on the user's machine that would bypass the security settings of their browser.

We have not yet received reports of anyone actually being attacked with this exploit. However, RealNetworks, has found and fixed the problem.
The first bug is essentially a parsing error in the jukebox code associated with reading RJS skin files, commonly known as a "buffer overrun" bug which could theoretically be used by hackers to adversely affect users. The bug was fixed by improving the robustness of skin file parsing. When RealJukebox encounters files modified in the manner described by this exploit, it will ignore the corrupt information in the skin, and switch to the skin as specified.
The second bug is a problem in the skin loading mechanism for RealJukebox 2 where files are extracted to known locations. This issue was fixed by increasing dynamic nature of the extraction locations.

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/bufferoverrun07092002.html

- **15133 RealOne Player / RealPlayer 8 / RealPlayer Intranet 8 Multiple Vulnerabilities (Remote File Checking)**
  The specific exploit, involves the View Clip Source feature of RealPlayer on multi-user systems.
  We have not yet received reports of anyone actually being attacked with this exploit. However, RealNetworks has found and fixed the problem.
  The vulnerability exists in multi-user systems, when the View Clip Source capability on a local file is accessed and the user subsequently leaves the RealPlayer running. In these circumstances, another user on the same system could potentially connect to the running player and use View Clip Source to gain read-access to files in which RealPlayer has been authorized to play back.
  This vulnerability has been fixed. Currently, content in the RealPlayer file format that has been played and viewed in an active RealPlayer session will be allowed to be viewed again by another user.

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

CVE Link: GENERIC-MAP-NOMATCH

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

- **15287 RealOne Player / RealPlayer 8 / RealPlayer 7 / RealPlayer G2 / RealPlayer Intranet 8 / RealPlayer Intranet 7 Multiple Vulnerabilities (Remote File Checking)**
  The specific exploit, commonly known as a "buffer overrun", could allow an attacker to run arbitrary code on a user's machine.

  We have not yet received reports of anyone actually being attacked with this exploit. However, RealNetworks, has found and fixed the problem.

  The bug is essentially a parsing error in the player code associated with reading RM files, commonly known as a "buffer overrun" bug which could theoretically be used by hackers

to adversely affect users. The bug was fixed by improving the robustness of file parsing. When RealPlayer encounters files modified in the manner described by this exploit, it will now inform the user that the file is corrupt when played.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: M**edium**

CVE Link: GENERIC-MAP-NOMATCH

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

- **19296 Hijack Possible Browser Hijack attempt**

  Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Low**

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/PestInfo/r/rightfinder.asp

- **19297 Hijack PowerSearch**

  Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Low**

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/PestInfo/p/possible_browser_hijack_attempt.asp

- **19298 Hijack RightFinder**

  Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Low**

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/PestInfo/p/powersearch.asp

New Vulnerabilities found this Week

- **Microsoft Word Document Parsing Buffer Overflow Vulnerability**
  "Denial of Service"
  HexView has discovered a vulnerability in Microsoft Word, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a user's system.
  The vulnerability is caused due to an input validation error within the parsing of document files and may lead to a stack-based buffer overflow.
  This can be exploited to crash the process when the user opens a specially crafted document. However, due to the nature of the problem, execution of arbitrary code may potentially also be possible, though it has not been proven.

  References: http://secunia.com/advisories/12758/

- **BlackBoard Internet Newsboard System Arbitrary File Inclusion**
  "Include arbitrary files from external and local resources"
  Cracklove has reported a vulnerability in BlackBoard Internet Newsboard System, which can be exploited by malicious people to compromise a vulnerable system.
  Input passed to the "libpach" parameter in "checkdb.inc.php" is not properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources.
  Example:
  http://[victim]/bb_lib/checkdb.inc.php?libpach=[malicious_URL]
  It is reportedly also possible to disclose the full path to certain scripts by accessing them directly.
  The vulnerability has been reported in version 1.5.1. Prior versions may also be affected.

  References: http://blackboard.unclassified.de/70,1#1031

- **AWS MySQLguest Script Insertion Vulnerability**
  "Script insertion attacks"
  BliZZard has reported a vulnerability in AWS MySQLguest, which can be exploited by malicious people to conduct script insertion attacks.
  Input passed to the "Name", "Email", "Homepage", and "Comments" fields is not properly sanitised before being used. This can be exploited to inject arbitrary HTML and script code, which will be executed in a user's browser session in context of an affected site when the malicious guestbook entry is viewed.

  References: http://secunia.com/advisories/12732/

- **Mac OS X Security Update Fixes Multiple Vulnerabilities**
  "Various vulnerabilities"
  Apple has issued a security update for Mac OS X, which fixes various vulnerabilities.
  1) A vulnerability in the AFP Server can be exploited by guest users to disconnect AFP volumes by sending specially crafted SessionDestroy packets.
  The vulnerability does reportedly not affect versions prior to 10.3.
  2) A security issue in the AFP Server can be exploited to change the permissions of a write-only AFP drop box to read-write due to an incorrect setting of the guest group id.

This problem does reportedly not affect versions prior to 10.3.
3) A vulnerability in CUPS can be exploited by malicious people to cause a DoS (Denial of Service).
4) A vulnerability in CUPS within certain methods of authenticated remote printing can be exploited to disclose users' passwords in the log files.
5) A security issue in the NetInfo Manager utility may result in an incorrect indication of the "root" account being disabled.
This problem does reportedly not affect versions prior to 10.3.
6) A security issue in postfix with "SMTPD AUTH" enabled may result in only users with the longest usernames being able to authenticate.
This problem does reportedly not affect versions prior to 10.3.
7) A vulnerability in QuickTime can potentially be exploited to compromise a user's system. The vulnerability is caused due to a boundary error within the handling of BMP images.
8) ServerAdmin comes with a self signed default certificate used for encrypted communication. However, this certificate is the same on all systems and it is therefore possible to decrypt and read captured sessions if this certificate is used.

References:
http://www.apple.com/support/dow...40930macosx1035clientserver.html
http://www.apple.com/support/dow...30macosx1028clientandserver.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