netVigilance

**ScoutNews Team** **5 November 2004**
**Issue #45**

Weekly ScoutNews by netVigilance

**Table of Contents**



# This Week in Review

Now you can be Phished just by opening an email – take that!
Microsoft will be pre-announcing the amount of patches coming down the line in an effort to make big and small feel treated the same.
There is an interesting trend where Cyber and Physical security are beginning to converge

Enjoy reading

# Top Security News Stories this Week

### ❖ Phishers Adopt Scam Tricks From Virus Writers

You know all about phishing scams, right? You know better than to click on a Web link embedded in an e-mail that purports to be from your bank, or to reply to messages requesting your user name and password. But if you think that's enough to protect yourself, think again. A phishing scam currently spreading online works without your ever having to click on a link; all that's required to activate the scam is for you to open an e-mail. And, many security experts warn, this threat may be a sign of things to come.
http://story.news.yahoo.com/news?tmpl=story&cid=1093&ncid=738&e=5&u=/pcworld/20041105/tc_pcworld/118489
Liane Cassavoy and Andrew Brandt, PC World

### ❖ Microsoft to Warn of Security Flaws

Criticized for a program that only provided some of its largest customers with warnings on security problems in its products, Microsoft Corp. now says it will give all computer users early word on such issues.
Beginning this month, the Redmond software giant will make public in advance how many security fixes it plans to release in its regular monthly bulletin, how severe the problems are and what products are affected.
http://story.news.yahoo.com/news?tmpl=story&cid=562&ncid=738&e=2&u=/ap/20041105/ap_on_hi_te/microsoft_security
AP

### ❖ Network Security Gets Physical

Physical security begins to meld with cyber security
When you hear about convergence, it's usually in reference to the union of voice and data networks. But the security sector is about to witness its own version of this phenomenon as

more customers begin to demand ways to make their networks and physical security systems work better together.
The need is being driven partly by the heightened focus on overall security since the creation of the Department of Homeland Security and the establishment of regulations such as HIPAA and Sarbanes-Oxley, as well as by the availability of network-monitoring tools that centralize the administration of disparate systems.
That doesn't necessarily mean mom-and-pop hardware stores will have their networks, security cameras and alarm systems running from one centralized console, or that security guards and IT personnel will be interchangeable any time soon. But the roles of these employees are beginning to overlap like never before, and, typically, the organizations looking most closely at these technologies are primarily found in the government, banking and health-care sectors.
http://www.varbusiness.com/sections/technology/tech.jhtml%3Bjsessionid=ALHACEL2PTOKWQSNDBCCKH0CJUMEKJVN?articleId=51200143
Luc hatlestad, VAR Business

# New Vulnerabilities Tested in SecureScout

- **13206 RealPlayer (10.5/10.5 Beta/10) / RealOne Player (v2/v1) Multiple Vulnerabilities (Remote File Checking)**

RealNetworks, Inc. has addressed a recently discovered security vulnerability that offered the potential for an attacker to run arbitrary or malicious code on a customer's machine.
The specific exploit was:
To fashion a malicious skin file to cause a buffer overflow which could have allowed an attacker to execute arbitrary code on a customer's machine. The buffer overrun was designed to occur in a 3rd-party compression library, DUNZIP32.DLL.
Skins files from RealNetworks' site are carefully examined before posting for viruses and exploits.

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

**CVE Links:** GENERIC-MAP-NOMATCH

**Reference:** http://www.nextgenss.com/advisories/realra3.txt &
http://service.real.com/realplayer/security/ &
http://www.service.real.com/help/faq/security/041026_player/EN/

- **14472 Mozilla / Thunderbird Valid Email Address Enumeration Weakness (Remote File Checking)**

plonk has discovered a weakness in Mozilla and Thunderbird, which can be exploited by malicious people to enumerate valid email addresses.

The weakness is caused due to an improper behaviour where references to external stylesheets in HTML documents are followed. This can be exploited to validate the existence of an mail address when a malicious mail is opened.

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

**CVE Links:** GENERIC-MAP-NOMATCH

**Reference:** http://secunia.com/advisories/13086/ & http://www.mozilla.org/security/ &

http://www.mozilla.org/press/mozilla-2004-10-01-02.html

- **14473 Internet Explorer IFRAME Buffer Overflow Vulnerability (Remote File Checking)**

  The vulnerability is caused due to a boundary error in the handling of certain attributes in the <IFRAME> HTML tag. This can be exploited to cause a buffer overflow via a malicious HTML document containing overly long strings in the "SRC" and "NAME" attributes of the <IFRAME> tag.

  Successful exploitation allows execution of arbitrary code.

  NOTE: This advisory has been rated "Extremely critical" as a working exploit has been published on public mailing lists.

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

**CVE Links:** GENERIC-MAP-NOMATCH

**Reference:** http://secunia.com/advisories/12959/ & http://www.securityfocus.org/bid/11515/ & http://felinemenace.org/~nd/crash_ie/ & http://lists.netsys.com/pipermail/full-disclosure/2004-November/028286.html

- **14667 WinRAR Repair Archive Feature Vulnerability (Remote File Checking)**

  Peter Winter-Smith of NGSSoftware has reported a vulnerability in WinRAR, which can be exploited by malicious people to compromise a user's system.
  The vulnerability is caused due to an error in the "Repair Archive" feature.
  Successful exploitation requires that a user is tricked into using the "Repair Archive" feature on a specially crafted archive file.

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

**CVE Link:** GENERIC-MAP-NOMATCH

**Reference:** http://secunia.com/advisories/13070/ & http://www.nextgenss.com/advisories/winrar.txt

- **15535 Cisco IOS OSPF Exploit (CSCdp58462)**

  The Open Shortest Path First (OSPF) implementation in certain Cisco IOS® software versions is vulnerable to a denial of service if it receives a flood of neighbor announcements in which more than 255 hosts try to establish a neighbor relationship per interface.

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

**CVE Link:** CAN-2003-0100

**Reference:**
http://www.cisco.com/en/US/tech/tk365/tk480/technologies_security_advisory09186a008014ac50.shtml & http://www.securityfocus.com/archive/1/312510

- **15556 Scanning for SSH Can Cause a Crash (CSCdv85279/CSCdw59394)**
  When an attacker tries to exploit the vulnerability VU#945216 the SSH module will consume too much of the processor's time, effectively causing a DoS.

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

**CVE Link:** CVE-2002-1024

**Reference:**
http://www.cisco.com/en/US/products/products_security_advisory09186a008009fafa.shtml

- **15557 Cisco VPN 3000 Concentrator Multiple Vulnerabilities (CSCdv88230/CSCdw22408)**
  The Cisco VPN 3000 series concentrators are a family of purpose-built, remote access Virtual Private Network (VPN) platforms for data encryption and authentication.

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

**CVE Link:** CAN-2002-1096

**Reference:**
http://www.cisco.com/en/US/products/products_security_advisory09186a00800c8154.shtml

- **15558 Cisco VPN 3000 Concentrator Multiple Vulnerabilities (CSCdx07754/CSCdx24622/CSCdx24632)**
  The Cisco VPN 3000 series concentrators are a family of purpose-built, remote access Virtual Private Network (VPN) platforms for data encryption and authentication.

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

**CVE Link:** CAN-2002-1100 & CAN-2002-1098

**Reference:** http://www.cisco.com/warp/public/707/vpn3k-multiple-vuln-pub.shtml

- **15559 Multiple Vulnerabilities in Access Control List Implementation for Cisco 12000 Series Internet Router (CSCdm44976/CSCdu57417/CSCdu03323/CSCdu35175/CSCdt96370/CSCdt69741)**
  Six vulnerabilities were found in IOS releases that are supporting Cisco 12000 platforms. Only line cards based on Engine 2 are affected.

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

**CVE Link:** CVE-2001-0862 & CVE-2001-0863 & CVE-2001-0864 & CVE-2001-0865 & CVE-2001-0866 & CVE-2001-0867

**Reference:** http://www.cisco.com/warp/public/707/GSR-ACL-pub.shtml

- **17926 Apache 2 Space Headers Denial of Service Vulnerability**

  Chintan Trivedi has discovered a vulnerability in Apache, which can be exploited by malicious people to cause a DoS (Denial of Service).
  The vulnerability is caused due to an error in the parsing routine for headers with a large amount of spaces. This can be exploited by sending some specially crafted requests with a large amount of overly long headers containing only spaces.
  Successful exploitation can cause the server to become unreachable and use a large amount of CPU resources, but will regain functionality once the attack stops.

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

**CVE Link:** GENERIC-MAP-NOMATCH

**Reference:** http://secunia.com/advisories/13045/ &
http://seclists.org/lists/fulldisclosure/2004/Nov/0022.html

# New Vulnerabilities found this Week

- **Mozilla / Thunderbird Valid Email Address Enumeration Weakness**

  "Validate the existence of an mail address"

plonk has discovered a weakness in Mozilla and Thunderbird, which can be exploited by malicious people to enumerate valid email addresses.
The weakness is caused due to an improper behavior where some references to external resources in HTML documents are followed. This can be exploited to validate the existence of an mail address when a malicious mail is opened using e.g. references to external stylesheets.
The weakness has been confirmed in Mozilla 1.7.3 and Thunderbird 0.8. Other versions may also be affected.

References: https://bugzilla.mozilla.org/show_bug.cgi?id=28327

- **WinRAR "Repair Archive" Feature Vulnerability**

Peter Winter-Smith of NGSSoftware has reported a vulnerability in WinRAR, which can be exploited by malicious people to compromise a user's system.
The vulnerability is caused due to an error in the "Repair Archive" feature.
Successful exploitation requires that a user is tricked into using the "Repair Archive" feature on a specially crafted archive file.
The vulnerability has been reported in versions 3.40 and prior.

References: http://www.nextgenss.com/advisories/winrar.txt

- **Cisco Secure ACS EAP-TLS User Authentication Bypass Vulnerability**

  "Bypass the user authentication"

A vulnerability has been reported in Cisco Secure Access Control Server and Cisco Secure ACS Solution Engine, which can be exploited by malicious people to bypass the user authentication.
The problem is that it is possible to be authenticated via an invalid, cryptographically correct certificate (e.g. comes from an untrusted CA or has expired) as long as a valid user name is

used.
Successful exploitation may allow bypassing user authentication, but requires that the device is configured to use EAP-TLS (Extensible Authentication Protocol-Transport Layer Security).
Also, exploitation has no impact on user authentication, if EAP-TLS is configured with binary comparison of user certificates as the only comparison method and if the user entry in Lightweight Directory Access Protocol/Active Directory (LDAP/AD) contains only valid certificates.
The vulnerability affects version 3.3.1 of the Cisco Secure ACS for Windows and Cisco Secure ACS Solution Engine.

References: http://www.cisco.com/en/US/produ...y_advisory09186a008033320e.shtml

- **Internet Explorer IFRAME Buffer Overflow Vulnerability**

"Execution of arbitrary code."
A vulnerability has been reported in Internet Explorer, which can be exploited by malicious people to compromise a user's system.
The vulnerability is caused due to a boundary error in the handling of certain attributes in the <IFRAME> HTML tag. This can be exploited to cause a buffer overflow via a malicious HTML document containing overly long strings in the "SRC" and "NAME" attributes of the <IFRAME> tag.
Successful exploitation allows execution of arbitrary code.
The vulnerability has been confirmed in the following versions:
* Internet Explorer 6.0 on Windows XP SP1 (fully patched).
* Internet Explorer 6.0 on Windows 2000 (fully patched).
NOTE: This advisory has been rated "Extremely critical" as a working exploit have been published on public mailing lists.

References: http://www.kb.cert.org/vuls/id/842160

- **Sun Java System Web Proxy Server Unspecified Buffer Overflow Vulnerabilities**

"Denial of Service"
Pentest Limited has reported some vulnerabilities in Sun Java System Web Proxy Server, which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.
The vulnerabilities are caused due to some unspecified boundary errors that can be exploited to cause buffer overflows.
The vulnerabilities affect Sun Java System Web Proxy Server 3.6 Service Pack 4 and prior.

References: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57606-1

**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