netVigilance

**ScoutNews Team**

**May 13 2005**
**Issue # 19**

Weekly ScoutNews by netVigilance

**Table of Contents**

# This Week in Review

Wumark worm spreading with image of famous albino gorilla.

Some security pointers from the Secret Service and CA. Dept of consumer affairs.

Content filtering systems rendered scap by new Phishing techniques.

IPSec flaw exposes VPN connections.

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

- **Wurmark Worm spreading by exploiting albino Gorilla story.**

The Wumark-K worm is spreading via an email attachment with either the subject lines; “Hehehe LOL!!” or “Your Photo Is On A Webpage!! “ as reported by SophosLabs™.

This is a malicious worm that invades systems to steal personal information. It is highly recommended that you have your virus scanning software updated with the latest signature files.

Sophos

Related Links :

http://www.sophos.com/virusinfo/articles/wurmarkk.html http://www.scmagazine.com/news/index.cfm?fuseaction=newsDetails&newsUID=6e950c64-8375-435f-a660-c87dfaa01c95&newsType=News

- **Secret Service and Ca. Dept. of Consumer Affairs outline cyber crime trends and describe best practices.**

Encrypted data, personal information are targets of professional organized criminals. Phishing / Pharming techniques are getting more devious in order to circumvent security measures. Some good antidotes on developing effective security policies.

Government Technology

http://www.govtech.net/news/news.php?id=93992

- **Phishers nullify content filtering with new tricks**

Phishers seem to be one step ahead of content-filtering vendors. The more sophisticated phishers will replace text with similar-looking images to slip through firewalls and content filters. Netcraft goes on to offer help in detecting these ‘undetectable’ sites.

netcraft

http://news.netcraft.com/archives/2005/05/12/fraudsters_seek_to_make_phishing_sites_undetectable_by_content_filters.html

- **Flaw in IPSec encryption and tunneling exposes VPN networks**

Britain's national emergency response team, the National Infrastructure Security Coordination Centre, discovered a vulnerability in the popular protocol, allowing an attacker to intercept and decrypt supposedly secure transmissions.

CNET News.com

http://news.com.com/Flaw+found+in+VPN+crypto+security/2100-1002_3-5705185.html?tag=nefd.top

# New Vulnerabilities Tested in SecureScout

- **14478 Adobe SVG Viewer libpng Vulnerability (Remote File Checking)**

A vulnerability has been reported in Adobe SVG Viewer, which can be exploited by malicious people to potentially compromise it.

An error in libpng can potentially be exploited to execute arbitrary code on a user's system via a specially crafted PNG image.

The vulnerability affects version 3.01 and prior.

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

**References:**

http://www.hyperdose.com/advisories/H2005-07.txt
http://secunia.com/advisories/15255/

**CVE Reference:** CAN-2004-0597

### ❖ 14479 Adobe SVG Viewer Local File Detection Vulnerability (Remote File Checking)

A weakness has been reported in Adobe SVG Viewer, which can be exploited by malicious people to enumerate files on a user's system.

An error in the ActiveX control (NPSVG3.dll) makes it possible for malicious web pages to determine whether or not a particular file exists on a user's system by specified the particular file in the "src" property.

The weakness affects versions 3.02 and prior.

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

**References:**

http://www.hyperdose.com/advisories/H2005-07.txt
http://secunia.com/advisories/15255/

**CVE Reference:** CAN-2004-0597

### ❖ 15186 Ethereal JXTA Protocol Dissector Vulnerabilities (Remote File Checking)

A vulnerability has been reported in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

An unspecified error in the JXTA dissector can be exploited to crash Ethereal.

This vulnerability affects version 0.10.9.

Test Case Impact: **Gather Info.** Vulnerability Impact: **High** Risk: **DoS, Buffer ovfl.**

**References:**

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00018.html

Product:
http://www.ethereal.com/

Other references:
http://security.lss.hr/en/index.php?page=details&ID=LSS-2005-03-04
http://security.lss.hr/en/index.php?page=details&ID=LSS-2005-03-05
http://secunia.com/advisories/14540/

**CVE Reference:** CAN-2005-0699, CAN-2005-0704, CAN-2005-0705, CAN-2005-0739, CAN-2005-0765, CAN-2005-0766

- **15187 Ethereal sFlow Protocol Dissector Vulnerabilities (Remote File Checking)**

A vulnerability has been reported in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

An unspecified error in the sFlow dissector can be exploited to crash Ethereal.

This vulnerability affects versions 0.9.14 through 0.10.9.

Test Case Impact: **Gather Info.** Vulnerability Impact: **High** Risk: **DoS, Buffer ovfl.**

**References:**

Original Advisory:
http://www.ethereal.com/appnotes/enpa-sa-00018.html

Product:
http://www.ethereal.com/

Other references:
http://security.lss.hr/en/index.php?page=details&ID=LSS-2005-03-04
http://security.lss.hr/en/index.php?page=details&ID=LSS-2005-03-05
http://secunia.com/advisories/14540/

**CVE Reference:** CAN-2005-0699, CAN-2005-0704, CAN-2005-0705, CAN-2005-0739, CAN-2005-0765, CAN-2005-0766

- **15188 Vulnerability in Web View Could Allow Remote Code Execution (MS05-024/894320) (Remote File Checking)**

A vulnerability has been reported in iTunes, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error within the MPEG-4 file parsing and can be exploited to cause a buffer overflow via a specially crafted MPEG-4 file.

Successful exploitation may allow execution of arbitrary code.

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

**References:**

Original Advisory:
http://docs.info.apple.com/article.html?artnum=301596

Product:
http://www.apple.com/itunes/

Other references:
http://secunia.com/advisories/15310/

**CVE Reference:** CAN-2005-1248

### ❖ 15189 Vulnerability in Web View Could Allow Remote Code Execution (MS05-024/894320) (Remote File Checking)

A remote code execution vulnerability exists in the way that Web View in Windows Explorer handles certain HTML characters in preview fields. By persuading a user to preview a malicious file, an attacker could execute code. However, user interaction is required to exploit this vulnerability.

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

**References:**

http://www.microsoft.com/technet/security/Bulletin/MS05-024.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1191

**CVE Reference:** CAN-2005-1191

### ❖ 15190 Mozilla Firefox Download Dialog Spoofing Vulnerability (Remote File Checking)

Secunia Research has discovered a vulnerability in Mozilla Firefox, which can be exploited by malicious people to spoof file types in the file download dialog.

The filename and the "Content-Type" header are not sufficiently validated before being displayed in the file download dialog. This can be exploited to spoof file types in the file download dialog by sending specially crafted headers containing white spaces, dots, and ASCII bytes 160.

Successful exploitation may trick a user into executing malware if the file is opened through the file download dialog.

The vulnerability has been confirmed in Mozilla Firefox 0.10.1 AND 1.0 for Windows. Other versions may also be affected.

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

**References:**

Original Advisory:
http://secunia.com/secunia_research/2004-11/advisory/

Product HomePage:
http://www.mozilla.org/products/firefox/

Other references:
https://bugzilla.mozilla.org/show_bug.cgi?id=267122
https://bugzilla.mozilla.org/show_bug.cgi?id=267123
https://bugzilla.mozilla.org/show_bug.cgi?id=275441
http://secunia.com/advisories/12979/

**CVE Reference:** None

### ❖ 15191 Mozilla Firefox Download Dialog Spoofing and Malware Execution Vulnerability (Remote File Checking)

Secunia Research has discovered a vulnerability in Mozilla Firefox, which can be exploited by malicious people to spoof file types in the file download dialog.

The "Content-Type" header is used for associating a file to a file type in the file download dialog, but the file extension is left intact when saving the file to disk with "Save to Disk". This can be exploited to spoof file types in the file download dialog.

Successful exploitation may result in malware being saved to the download directory, which by default is the desktop.

NOTE: If the downloaded malware is a shortcut or some executable file, then the icon can be spoofed in the download manager and on the desktop.

The vulnerability has been confirmed in Mozilla Firefox 1.0 for Windows. Other versions may also be affected.

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

**References:**

Original Advisory:
http://secunia.com/secunia_research/2004-11/advisory/

Product HomePage:
http://www.mozilla.org/products/firefox/

Other references:
https://bugzilla.mozilla.org/show_bug.cgi?id=267122
https://bugzilla.mozilla.org/show_bug.cgi?id=267123
https://bugzilla.mozilla.org/show_bug.cgi?id=275441
http://secunia.com/advisories/12979/

**CVE Reference:** None

### ❖ 15192 Netscape HTTP Authentication Prompt Spoofing Vulnerability (Remote File Checking)

A vulnerability has been reported in Netscape, which can be exploited by malicious people to spoof HTTP authentication prompts.

The vulnerability has been confirmed in version 7.2. Other versions may also be affected.

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

**References:**

Original Advisory:
http://www.networksecurity.fi/advisories/netscape-auth.html

Product HomePage:
http://channels.netscape.com/ns/browsers/default.jsp

Other references:
http://secunia.com/advisories/14407/
http://secunia.com/advisories/15267/

**CVE Reference:** None

### ❖ 15193 Mozilla Firefox "IFRAME" JavaScript URLs Vulnerability (Remote File Checking)

A vulnerability has been discovered in Firefox, which can be exploited by malicious people to conduct cross-site scripting attacks and compromise a user's system.

The problem is that "IFRAME" JavaScript URLs are not properly protected from being executed in context of another URL in the history list. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an arbitrary site.

The vulnerability has been confirmed in version 1.0.3. Other versions may also be affected.

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

**References:**

Original Advisory:

http://www.mozilla.org/security/announce/mfsa2005-42.html

Product HomePage:

http://www.mozilla.org/products/firefox/

Other references:

http://www.kb.cert.org/vuls/id/534710

http://www.kb.cert.org/vuls/id/648758

http://secunia.com/advisories/15292/

**CVE Reference:** CAN-2005-1476, CAN-2005-1477

# New Vulnerabilities found this Week

- **iTunes MPEG-4 File Parsing Buffer Overflow Vulnerability**
  "Execution of arbitrary code"

  A vulnerability has been reported in iTunes, which potentially can be exploited by malicious people to compromise a user's system.

  The vulnerability is caused due to a boundary error within the MPEG-4 file parsing and can be exploited to cause a buffer overflow via a specially crafted MPEG-4 file.

  Successful exploitation may allow execution of arbitrary code.

References:
http://docs.info.apple.com/article.html?artnum=301596

- **Microsoft Windows Explorer Web View Script Insertion Vulnerability**
  “Execution of arbitrary code”

  GreyMagic has discovered a vulnerability in Windows, which can be exploited by malicious people to compromise a user's system.

  The vulnerability is caused due to an input validation error in the Web View library "webvw.dll" where certain metadata for files isn't properly sanitized before being used. This can be exploited to execute arbitrary HTML and script code in a local context with escalated privileges by e.g. tricking a user into selecting a malicious word document with a specially crafted author name in Windows Explorer.

  Successful exploitation allows execution of arbitrary code.

  The vulnerability has been confirmed on a fully patched Microsoft Windows 2000 SP4 system.

  References:
  http://www.greymagic.com/security/advisories/gm015-ie/
  http://www.microsoft.com/technet/security/Bulletin/MS05-024.mspx

- **Bugzilla Two Information Disclosure Weaknesses**
  “Gain knowledge of sensitive information”

  Two weaknesses have been reported in Bugzilla, which can be exploited by malicious users to gain knowledge of sensitive information.

  1) Users can determine whether or not a given invisible product exists, as an access denied error is returned when the user attempts to access a valid product.

  Users can also enter bugs into products closed for bug entry, if a valid product name is known.

  This weakness affects versions 2.10 through 2.18, 2.19.1, and 2.19.2.

  2) A user's password may be embedded as part of a report URL, which causes it to be visible in the web logs.

  This weakness affects versions 2.17.1 through 2.18, 2.19.1, and 2.19.2.

  References:
  http://www.bugzilla.org/security/2.16.8/
  https://bugzilla.mozilla.org/show_bug.cgi?id=287109

https://bugzilla.mozilla.org/show_bug.cgi?id=287436

- **Mozilla Firefox Download Dialog Spoofing Vulnerabilities**
"Spoof file types in the file download dialog"

Secunia Research has discovered two vulnerabilities in Mozilla Firefox, which can be exploited by malicious people to spoof file types in the file download dialog.

1) The filename and the "Content-Type" header are not sufficiently validated before being displayed in the file download dialog. This can be exploited to spoof file types in the file download dialog by sending specially crafted headers containing white spaces, dots, and ASCII bytes 160.

Successful exploitation may trick a user into executing malware if the file is opened through the file download dialog.

The vulnerability has been confirmed in Mozilla Firefox 0.10.1 for Windows. Other versions may also be affected.

2) The "Content-Type" header is used for associating a file to a file type in the file download dialog, but the file extension is left intact when saving the file to disk with "Save to Disk". This can be exploited to spoof file types in the file download dialog.

Successful exploitation may result in malware being saved to the download directory, which by default is the desktop.

NOTE: If the downloaded malware is a shortcut or some executable file, then the icon can be spoofed in the download manager and on the desktop.

The vulnerability has been confirmed in Mozilla Firefox 1.0 for Windows. Other versions may also be affected.

References:
https://bugzilla.mozilla.org/show_bug.cgi?id=267122
https://bugzilla.mozilla.org/show_bug.cgi?id=267123
https://bugzilla.mozilla.org/show_bug.cgi?id=275441

- **Gaim URL Processing Buffer Overflow Vulnerability**
"Denial of Service"

A vulnerability and a weakness have been reported in Gaim, which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a user's system.

1) A boundary error within the processing of messages containing URLs can be exploited to cause a stack-based buffer overflow via a message containing an overly long URL (more than 8192 bytes).

Successful exploitation allows execution of arbitrary code.

2) A NULL pointer dereference error within the handling of MSN messages can be exploited to crash the application via a SLP message with an empty body.

References:
http://gaim.sourceforge.net/security/index.php?id=16
http://gaim.sourceforge.net/security/index.php?id=17
http://rhn.redhat.com/errata/RHSA-2005-429.html

- **Sun Solaris automountd Denial of Service Vulnerability**
  "Denial of Service"

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

The vulnerability is caused due to an unspecified error and can be exploited to stop automountd by accessing "/xfn/_x500".

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57786-1

- **libTIFF BitsPerSample Tag Buffer Overflow Vulnerability**
  "Execution of arbitrary code"

Tavis Ormandy has reported a vulnerability in libTIFF, which potentially can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error and can be exploited to cause a buffer overflow via a specially crafted TIFF image containing a malformed BitsPerSample tag.

Successful exploitation may allow execution of arbitrary code, if a malicious TIFF image is opened in an application linked against the vulnerable library.

References:
http://bugzilla.remotesensing.org/show_bug.cgi?id=843
http://security.gentoo.org/glsa/glsa-200505-07.xml

**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