netVigilance

ScoutNews Team

January 7th 2005
Issue # 1

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Welcome to the first edition of ScoutNews of 2005

This year will with no doubt bring many new changes.

1. Large companies merging to try to beat each other to the pinnacle of the one stop security shop. This week we are bringing a story about the merger of Symantec and Veritas.
2. We are also seeing that Nessus is not really freeware anymore – causing myriad of companies that have built businesses based on this service being free now needing to look other places for solutions.

Now is the time you should call or email netVigilance to get an update on SecureScout. (503) 524 5758 or sales@netVigilance.com

Enjoy reading

Top Security News Stories this Week

- **Symantec & Veritas CEOs detail merger**

The merger between Symantec and Veritas and their respective security and storage management technologies will meet the evolving needs of enteprise security managers, Veritas Chairman, President and CEO Gary Bloom said.
Security managers have become IT risk managers, responsible for regulatory compliance and system availability in addition to security, Bloom said. "You'll see more of that consolidated view in the future," he predicted.
http://www.scmagazine.com/news/index.cfm?fuseaction=newsDetails&newsUID=931f75f5-748f-4714-8b7d-f0327ca2eea6&newsType=Latest%20News
Marcia Savage

- **Nessus no longer free**

Vendors relying on open-source Nessus won't automatically get free, timely "plugin" programs after project managers of the popular vulnerability scanner announced a new feed structure that provides the most recent releases for a fee. The move comes after Nessus managers decided too many commercial users contributed nothing to the

collaborative program.
Though no company names were mentioned by Nessus leaders during their recent announcement, the popular vulnerability scanner reportedly is used in many commercial security products and services. A quick Internet search indicated some of those security vendors include StillSecure, VeriSign, IBM Global Services, Counterpane Internet Security, Symantec, AcuNett, ScannerX and rackAID, among others.
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1034903,00.html
Shawna McAlearney

- **Virus surprise hidden inside Christmas gifts**

Staff exhibiting their Christmas presents at work may find they give their company an unwanted New Year surprise. Reports today show MP3 players can shut down Windows by passing on the VBS/Soraci virus.
According to Kaspersky some MP3 players are arriving readily infected because they are tested on computer systems carrying the Soraci virus. Once these players are connected to a Windows 9x/ME PC it infects it.
http://www.scmagazine.com/news/index.cfm?fuseaction=newsDetails&newsUID=de14e866-0c05-4f9b-af78-82405d9d30d4&newsType=News
David Quainton

New Vulnerabilities Tested in SecureScout

- **14676 Mozilla Download Dialog Source Spoofing (Remote File Checking)**

Secunia Research has discovered a vulnerability in Mozilla, which can be exploited by malicious people to spoof the source displayed in the Download Dialog box.

The problem is that long sub-domains and paths aren't displayed correctly, which therefore can be exploited to obfuscate what is being displayed in the source field of the Download Dialog box.

The vulnerability has been confirmed in Mozilla 1.7.3 for Linux, Mozilla 1.7.5 for Windows. Other versions may also be affected.

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

CVE Links:

Reference: http://secunia.com/secunia_research/2004-15/advisory/ &
https://bugzilla.mozilla.org/show_bug.cgi?id=275417 &
http://www.mozilla.org/products/mozilla1.x/

- **14677 Mozilla Firefox Download Dialog Source Spoofing (Remote File Checking)**

Secunia Research has discovered a vulnerability in Mozilla Firefox, which can be exploited by malicious people to spoof the source displayed in the Download Dialog box.

The problem is that long sub-domains and paths aren't displayed correctly, which therefore can be exploited to obfuscate what is being displayed in the source field of the

Download Dialog box.

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

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

CVE Links:

Reference: http://secunia.com/secunia_research/2004-15/advisory/ & https://bugzilla.mozilla.org/show_bug.cgi?id=275417 & http://www.mozilla.org/products/firefox/

- **14678 Mozilla Browser Network News Transport Protocol Remote Heap Overflow Vulnerability (Remote File Checking)**

Mozilla is vulnerable to a heap overflow vulnerability against its nntp functionnality. This may allow an attacker to execute arbitrary code on the remote host.

To exploit this flaw, an attacker would need to set up a rogue news site and lure a victim on the remote host into reading news from it.

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

CVE Links:

Reference: http://www.securityfocus.com/archive/1/385709 & http://www.securityfocus.com/bid/12131 & http://xforce.iss.net/xforce/xfdb/18711

- **14679 Mozilla SOAPParameter Integer Overlow (Remote File Checking)**

Mozilla is vulnerable to an integer overflow in the SOAPParameter object constructor. An attacker may exploit this flow to corrupt the process memory and possibly to execute arbitrary code on the remote host.

To exploit this flaw, an attacker would need to set up a rogue website and lure a victim on the remote host into visiting it.

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

CVE Link: CAN-2004-0722

Reference: http://www.securityfocus.com/bid/10843 & https://bugzilla.mozilla.org/show_bug.cgi?id=236618 & http://www.mozilla.org/products/mozilla1.x/

- **14680 Mozilla/Firefox security manager certificate handling DoS (Remote File Checking)**

Mozilla Internet Browser Personal Security Manager (PSM) is reported prone to a vulnerability that may permit a remote malicious attacker to silently import an invalid certificate into the Mozilla Personal Security Manager certificate store.

An attacker may exploit this vulnerability to corrupt the Mozilla PSM certificate store and as a result deny HTTPS service.

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

CVE Link: CAN-2004-0758

Reference: http://www.securityfocus.com/bid/10703 &
http://www.mozilla.org/projects/security/known-vulnerabilities.html &
http://www.mozilla.org/products/mozilla1.x/

- **15152 Winamp Tag Processing Remote Denial Of Service Vulnerability (Remote File Checking)**

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

Winamp is reported prone to a remote denial of service vulnerability. The issue is reported to present itself when certain '.mp4' and '.m4a' files are processed.

It is not known at this point whether this vulnerability may be exploited to any means other than a denial of service.

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

CVE Link:

Reference: http://www.securityfocus.com/bid/11909 &
http://www.securityfocus.com/archive/1/384241

- **15153 Winamp Long File Name Denial of Service Vulnerability (Remote File Checking)**

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

It has been reported that Winamp may be prone to a denial of service vulnerability when processing files with a name exceeding 246 characters. Immediate consequences of this issue may result in the application crashing. Although unconfirmed, due to the nature of this vulnerability an attack could result in a buffer overflow condition and may lead to arbitrary code execution. Any code execution would occur in the context of the user running the application.

Winamp 5.02 was identified as the vulnerable version, however, it is possible that other versions are affected as well.

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

CVE Link:

Reference: http://www.securityfocus.com/archive/1/357986 &
http://www.securityfocus.com/archive/1/358097

- **15568 Exim 4.x - SPA Authentication Vulnerability**
  Exim is a Unix message transfer agent (MTA) developed at the University of Cambridge.

  Exim is vulnerable to a buffer overflow in the function spa_base64_to_bits(), which is part of the code for SPA authentication. This code originated in the Samba project. The overflow can be exploited only if you are using SPA authentication.

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

CVE Link: CAN-2005-0021 & CAN-2005-0022

Reference: http://www.exim.org/mail-archives/exim-announce/2005/msg00000.html

- **19312 Hijack SP Hijacker**
  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/s/sp_hijacker.asp

- **19313 Hijack SubSearch**
  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/s/subsearch.asp

New Vulnerabilities found this Week

- **Apache Tomcat "Tomcat Manager" Cross-Site Scripting.**
  "Cross-site scripting attacks"

  Oliver Karow has discovered some vulnerabilities in Apache Tomcat, which can be exploited by malicious people to conduct cross-site scripting attacks.

  Various input passed to the "Tomcat Manager" is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

Successful exploitation requires that the user has been authenticated.
The vulnerabilities have been confirmed in version 5.5.4. Other versions may also be affected.

References:
http://www.oliverkarow.de/research/jakarta556_xss.txt

❖ Apache mod_dosevasive Insecure Temporary File Creation

"Escalated privileges"

LSS Security Team has reported a weakness in mod_dosevasive for Apache, which can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges.

Temporary files are created insecurely and can be exploited via symlink attacks to create arbitrary files containing action trace log information on the system.

Combined with a minor race condition, this can potentially be exploited to overwrite existing files.

The vulnerability has been reported in versions 1.9 and prior.

References:
http://security.lss.hr/en/index.php?page=details&ID=LSS-2005-01-01

❖ Exim IPv6 Handling and SPA Authentication Vulnerabilities

"Gain escalated privileges"

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

1) A boundary error in the function "host_aton()" when handling IPv6 addresses may be exploited to cause a buffer overflow by supplying a specially crafted IPv6 address with more than 8 components to an unspecified command line option.

2) A boundary error in the function "spa_base64_to_bits()" when handling SPA authentication can be exploited to cause a buffer overflow.

Successful exploitation requires that SPA authentication is enabled.
References:
http://www.exim.org/mail-archives/exim-announce/2005/msg00000.html

❖ Bugzilla Internal Error Response Cross-Site Scripting

"Cross-site scripting attacks"

Michael Krax has reported a vulnerability in Bugzilla, which can be exploited by malicious people to conduct cross-site scripting attacks.

Input passed in HTTP requests is not properly sanitised before being returned to users in error messages when an internal error is encountered. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site.

References:
https://bugzilla.mozilla.org/show_bug.cgi?id=272620

- **Mozilla / Mozilla Firefox Download Dialog Source Spoofing**

“Spoofing”

Secunia Research has discovered a vulnerability in Mozilla / Mozilla Firefox, which can be exploited by malicious people to spoof the source displayed in the Download Dialog box.

The problem is that long sub-domains and paths aren't displayed correctly, which therefore can be exploited to obfuscate what is being displayed in the source field of the Download Dialog box.

The vulnerability has been confirmed in Mozilla 1.7.3 for Linux, Mozilla 1.7.5 for Windows, and Mozilla Firefox 1.0. Other versions may also be affected.

References:
http://secunia.com/secunia_research/2004-15/advisory/
https://bugzilla.mozilla.org/show_bug.cgi?id=275417

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