netVigilance

ScoutNews Team

February 11, 2005
Issue # 6

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Watch out for infectious chat, security holes introduced by security software and the threat of your car or refrigerator getting sick.

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

- **MSN Worm can Hijack your system.**

A new Internet worm is squirming through Microsoft Corp.'s popular MSN Messenger chat network, anti-virus vendors warned on Thursday

According to an advisory from F-Secure, the new W32/Bropia-A worm users MSN Messenger to lure users into downloading one of the following files: "Drunk_lol.pif"; "Webcam_004.pif"; "sexy_bedroom.pif"; "naked_party.pif"; or "love_me.pif."

Once executed, Bropia-A also drops a variant of the Rbot backdoor Trojan. Rbot represents the large family of backdoors fitted with the ability to control a victim's machine remotely.

eWeek

Full Story: http://www.eweek.com/article2/0,1759,1752988,00.asp

- ### Security Holes found in popular Network Security Products

Internet Security Systems (ISS) reported that their X-force research team has discovered a serious vulnerability in a Symantec parsing engine, which is used in several of the company's products. The vulnerability could allow arbitrary code to execute on a affected systems. ISS rates the vulnerability as critical.

More reason to implement overlapping ‘sets of eyes’ when it comes to protecting your digital assets.

WindowITPro

Full Story : http://www.windowsitpro.com/Article/ArticleID/45393/45393.html

- ### “I can’t make it into work today; my car has a virus”

In a survey published by IBM, mobile phones, handheld computers, wireless networks and yes, car engine control computers; are increasingly coming under attack from computer virus’.

Embedded controllers such as the types of systems that are prevalent in today’s cars, appliances, phones are susceptible to malicious attack.

The "Security Threats and Attack Trends Report" details past trends and future predictions on the state of digital security.

Computerworld

Full Story: http://www.computerworld.com/securitytopics/security/story/0,10801,99719,00.html?from=homeheads

New Vulnerabilities Tested in SecureScout

- **14687 ASP.NET Path Validation Vulnerability (MS05-004/887219) (Remote File Checking)**

The canonicalization routine that is used by ASP.NET to map the request does not correctly parse the URL and that could allow an attacker to bypass the security of an ASP.NET Web site and gain unauthorized access. An attacker who successfully exploited this vulnerability could take a variety of actions, depending on the specific contents of the website.

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

References: http://www.microsoft.com/technet/security/bulletin/MS05-004.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0847

CVE Reference: CAN-2004-0847

- ❖ **14688 Vulnerability in Microsoft Office XP could allow Remote Code Execution (MS05-005/873352) (Remote File Checking)**

A buffer overrun in the process that passes URL file locations to Microsoft Office XP software exists and that could allow remote code execution on an affected system. An attacker who successfully exploited this vulnerability could take complete control of the affected system.

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

References: http://www.microsoft.com/technet/security/bulletin/MS05-005.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0848

CVE Reference: CAN-2004-0848

CVE Reference:

- ❖ **14689 Vulnerability in Windows SharePoint Services and SharePoint Team Services Could Allow Cross-Site Scripting and Spoofing Attacks (MS05-006/887981) (Remote File Checking)**

This is a cross-site scripting and spoofing vulnerability. The affected software does not completely validate input that is provided to a HTML redirection query before it sends this input to the browser.

The cross-site scripting vulnerability could allow an attacker to convince a user to run a malicious script. If this malicious script is run, it would execute in the security context of the user. Attempts to exploit this vulnerability require user interaction. This vulnerability could allow an attacker access to any data on the affected systems that was accessible to the individual user.

It may also be possible for an attacker to exploit this vulnerability to modify Web browser caches and intermediate proxy server caches, and put spoofed content in those caches.

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

References: http://www.microsoft.com/technet/security/bulletin/MS05-006.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0049

CVE Reference: CAN-2005-0049

- **14690 Vulnerability in Windows Could Allow Information Disclosure (MS05-007/888302) (Remote File Checking)**

The process that is used by the affected software to validate authentication information when a client establishes an anonymous logon by using a named pipe connection introduces an information disclosure vulnerability.

An attacker who successfully exploited this vulnerability could remotely read the user names for users who have an open connection to an available shared resource.

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

References: http://www.microsoft.com/technet/security/bulletin/MS05-007.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0051

CVE Reference: CAN-2005-0051

- **14691 Vulnerability in Windows Shell Could Allow Remote Code Execution (MS05-008/890047) (Remote File Checking)**

A remote code execution vulnerability exists in Windows Media Player because it does not properly handle PNG files with excessive width or height values. An attacker could try to exploit the vulnerability by constructing a malicious PNG that could potentially allow remote code execution if a user visited a malicious Web site or clicked a link in a malicious e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A remote code execution vulnerability exists in Windows Messenger because it does not properly handle corrupt or malformed PNG files. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References: http://www.microsoft.com/technet/security/bulletin/MS05-008.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0053

CVE Reference: CAN-2005-0053

- **14692 Vulnerability in PNG Processing Could Allow Remote Code Execution (MS05-009/890261) (Remote File Checking)**

A remote code execution vulnerability exists in Windows Media Player because it does not properly handle PNG files with excessive width or height values. An attacker could try to exploit the vulnerability by constructing a malicious PNG that could potentially allow remote code execution if a user visited a malicious Web site or clicked a link in a malicious e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A remote code execution vulnerability exists in Windows Messenger because it does not properly handle corrupt or malformed PNG files. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References: http://www.microsoft.com/technet/security/bulletin/MS05-009.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1244
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0597

CVE Reference: CAN-2004-1244 CAN-2004-0597

❖ 14693 Vulnerability in the License Logging Service Could Allow Code Execution (MS05-010/885834) (Remote File Checking)

An unchecked buffer in the License Logging service exists and introduces a remote code execution vulnerability exists in the License Logging service that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

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

References:

CVE Reference:

❖ 14694 Vulnerability in Server Message Block Could Allow Remote Code Execution (MS05-011/885250) (Remote File Checking)

A remote code execution vulnerability exists in Server Message Block (SMB) that could allow an attacker who successfully exploited this vulnerable to take complete control of the affected system.

The vulnerability results because of the process that the affected operating systems use to validate certain incoming SMB packets.

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

References: http://www.microsoft.com/technet/security/bulletin/MS05-011.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0045

CVE Reference: CAN-2005-0045

❖ 14695 Vulnerability in OLE and COM Could Allow Remote Code Execution (MS05-012/873333) (Remote File Checking)

A privilege elevation vulnerability exists in the way that the affected operating systems and programs access memory when they process COM structured storage files. This vulnerability could allow a logged on user to take complete control of the system.

A remote code execution vulnerability exists in OLE because of the way that it handles input validation. An attacker could exploit the vulnerability by constructing a malicious document that could potentially allow remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, user interaction is required to exploit this vulnerability on Windows 2000, Windows XP, and Windows Server 2003.

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

References: http://www.microsoft.com/technet/security/bulletin/MS05-012.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0047
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0044

CVE Reference: CAN-2005-0047 CAN-2005-0044

- **14696 Vulnerability in the DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (MS05-013/891781) (Remote File Checking)**

A cross-domain vulnerability exists in the Microsoft Dynamic HTML (DHTML) Editing Component ActiveX control that could allow information disclosure or remote code execution on an affected system. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited that page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

References: http://www.microsoft.com/technet/security/bulletin/MS05-013.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1319

CVE Reference: CAN-2004-1319

- **14697 Vulnerability in the DHTML Editing Component ActiveX Control Could AlloCumulative Security Update for Internet Explorer (MS05-014/867282) (Remote File Checking)**

A privilege elevation vulnerability exists in Internet Explorer because of the way that Internet Explorer handles drag-and-drop events. An attacker could exploit the vulnerability by constructing a malicious Web page. This malicious Web page could potentially allow an attacker to save a file on the user's system if a user visited a malicious Web site or viewed a malicious e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, user interaction is required to exploit this vulnerability.

A remote code execution vulnerability exists in Internet Explorer because of the way that it handles certain encoded URLs. An attacker could exploit the vulnerability by constructing a malicious URL. This malicious URL could potentially allow remote code execution if a user visited a malicious Web site or viewed a malicious e-mail message. The URL could be made to look like a link to another Web site in an attempt to trick a user into clicking it. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, significant user interaction is required to exploit this vulnerability.

A remote code execution vulnerability exists in Internet Explorer because of the way that it handles certain DHTML methods. An attacker could exploit the vulnerability by constructing a malicious Web page. This malicious Web page could potentially allow remote code execution if a user visited a malicious Web site or viewed a malicious e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, user interaction is required to exploit this vulnerability.

A cross-domain vulnerability exists in Internet Explorer that could allow information disclosure or remote code execution on an affected system. An attacker could exploit the vulnerability by constructing a malicious Web page. The malicious Web page could potentially allow remote code execution if viewed by a user. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, significant 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/MS05-014.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0053
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0054
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0055
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0056

CVE Reference: CAN-2005-0053 CAN-2005-0054 CAN-2005-0055 CAN-2005-0056

❖ 14698 Vulnerability in Hyperlink Object Library Could Allow Remote Code Execution (MS05-015/888113) (Remote File Checking

A remote code execution vulnerability exists in the Hyperlink Object Library. This problem exists because of an unchecked buffer while handling hyperlinks. An attacker could exploit the vulnerability by constructing a malicious hyperlink which could potentially lead to remote code execution if a user clicks a malicious link within a Web site or e-mail message. An attacker who successfully exploited this vulnerability could take complete control of the affected system. 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/MS05-015.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0057

CVE Reference: CAN-2005-0057

New Vulnerabilities found this Week

F-Secure Multiple Products ARJ Archive Handling Vulnerability
“Buffer overflow”

ISS X-Force has reported a vulnerability in multiple F-Secure products, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the antivirus scanning functionality when processing ARJ archives. This can be exploited to cause a buffer overflow via a specially crafted ARJ archive.

Successful exploitation allows execution of arbitrary code, but requires that the malicious ARJ archive is scanned with archive scanning enabled.

References:
http://www.f-secure.com/security/fsc-2005-1.shtml
http://xforce.iss.net/xforce/alerts/id/188

Mailman "private.py" Directory Traversal Vulnerability
“Disclose sensitive information”

John Cartwright has reported a vulnerability in Mailman, which can be exploited by malicious people to disclose sensitive information.

The vulnerability is caused due to an input validation error in "private.py", making it possible to disclose the contents of arbitrary files via directory traversal attacks via the ".../....///" sequence.

The vulnerability has been reported in version 2.1.5. Other versions may also be affected.

Avaya krb5 Two Vulnerabilities
"Escalated privileges"

Avaya has acknowledged some vulnerabilities in krb5, which can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges and by malicious users to potentially compromise a vulnerable system.

The vulnerabilities affect:
* Avaya S8700/S8500/S8300 (CM2.0 and later)
* Avaya MN100 (All versions)
* Avaya Intuity LX (version 1.1 through 5.x)
* Avaya Modular Messaging MSS (All versions)

References:
http://support.avaya.com/elmodoc...y/ASA-2005-036_RHSA-2005-012.pdf

Symantec Multiple Products UPX Parsing Engine Buffer Overflow
"Boundary error"

ISS X-Force has reported a vulnerability in multiple Symantec products, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the DEC2EXE parsing engine used by the antivirus scanning functionality when processing UPX compressed files. This can be exploited to cause a heap-based buffer overflow via a specially crafted UPX file.

Successful exploitation allows execution of arbitrary code.

References:
http://www.sarc.com/avcenter/security/Content/2005.02.08.html

http://xforce.iss.net/xforce/alerts/id/187

ArGoSoft Mail Server Directory Traversal Vulnerabilities

"Disclose and manipulate sensitive information"

Tan Chew Keong has reported some vulnerabilities in ArGoSoft Mail Server, which can be exploited by malicious users to disclose and manipulate sensitive information, and potentially compromise a user's system.

1) An input validation error in the attachment handling can be exploited to create or overwrite arbitrary files via directory traversal attacks.

2) The problem is that the "_msgatt.rec" file, which holds information about uploaded files, can be overwritten by an uploaded attachment. This can be exploited to include arbitrary files as attachments in an mail via directory traversal attacks.

3) Input passed to the "Folder" parameter in "msg", "delete", "folderdelete" and "folderadd" isn't properly sanitised before being used. This can be exploited to access or delete mails for other currently logged on users, and create or delete arbitrary directories via directory traversal attacks.

The vulnerabilities have been reported in version 1.8.7.3 and prior.

References:
http://www.security.org.sg/vuln/argosoftmail1873.html

ArGoSoft FTP Server Compressed Shortcut Upload Security Bypass

"Bypass certain security restrictions"

Remus Hociota has reported a vulnerability in ArGoSoft FTP Server, which can be exploited by malicious users to bypass certain security restrictions.

The vulnerability is caused due to an error in the validation of shortcut (.lnk) files extracted from ZIP files via the "SITE UNZIP" command and can be exploited to access restricted resources.

Successful exploitation requires that "SITE UNZIP" command support is enabled.

References:
http://secunia.com/advisories/13063/

Mozilla / Firefox Three Vulnerabilities
"plant malware, cross-site scripting, bypass certain security restrictions"

mikx has discovered three vulnerabilities in Mozilla and Firefox, which can be exploited by malicious people to plant malware on a user's system, conduct cross-site scripting attacks and bypass certain security restrictions.

1) Mozilla and Firefox validate an image against the "Content-Type" HTTP header, but uses the file extension from the URL when saving an image after a drag and drop event. This can e.g. be exploited to plant a valid image with an arbitrary file extension and embedded script code (e.g. .bat file) on the desktop by tricking a user into performing a certain drag and drop event.

2) Missing URI handler validation when dragging a "javascript:" URL to another tab can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an arbitrary site by tricking a user into dragging a malicious link to another tab.

3) An error in the restriction of URI handlers loaded via plugins can be exploited to link to certain restricted URIs (e.g. about:config).

This can further be exploited to trick a user into changing some sensitive configuration settings.

The vulnerabilities have been confirmed in Mozilla 1.7.5 and Firefox 1.0. Other versions may also be affected.

References:
http://www.mikx.de/index.php?p=8

http://www.mikx.de/index.php?p=9
http://www.mikx.de/index.php?p=10

Mozilla / Firefox / Camino IDN Spoofing Security Issue

"spoof the URL displayed in the address bar, SSL certificate, and status bar"

Eric Johanson has reported a security issue in Mozilla / Firefox / Camino, which can be exploited by a malicious web site to spoof the URL displayed in the address bar, SSL certificate, and status bar.

The problem is caused due to an unintended result of the IDN (International Domain Name) implementation, which allows using international characters in domain names.

This can be exploited by registering domain names with certain international characters that resembles other commonly used characters, thereby causing the user to believe they are on a trusted site.

Secunia has constructed a test, which can be used to check if your browser is affected by this issue:

The issue has been confirmed in Mozilla 1.7.5 and Firefox 1.0. Other versions may also be affected.

References:
http://www.shmoo.com/idn/homograph.txt

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