ScoutNews Team **June 17, 2005**
Issue # 24

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Sneaky new Social Engineering attacks using Trojans discovered, wireless safeguards and DHS funds infrastructure security.

This is ScoutNews

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

- **UK Agency identifies Trojans being used in Social Engineering attacks.**

The U.K.'s National Infrastructure Security Co-Ordination Center discovered a series of attacks targeting specific organizations and individuals that have access to commercially or economically privileged information.

This represents a new form of cyber-attack that uses email messages with content of particular interest to the recipient. They will then either plant a Trojan or re-direct the victim to a site containing the Trojan.

Once in place; the Trojan covertly runs in the background to collect usernames, passwords, system information and even scans the hard drives.

Computerworld

Full Story :

http://www.computerworld.com/securitytopics/security/story/0,10801,102595,00.html

- **Tips for better Wi-Fi security**

Best practices advice on enhancing your wireless security, consider new encryption protocols such as LEAP, PEEP, AES or VPN for wireless networks.
InfoWorld

Full Story:
http://www.newsfactor.com/news/Wi-Fi-Security-Wakes-Up-to-Reality/story.xhtml?story_id=101009U6CKHZ

- **DHS to spend $11.7 million on research to secure critical infrastructure**

The money is earmarked for on research to secure the computer-aided control systems that operate the nation's critical infrastructure such as power plants, Dams, transmission systems, etc.

ScoutNews reported on this in issue #10, March 11th, 2005. "Nations power supply at risk from Hacker attack", tests conducted at the Idaho National Labs demonstrated the relative ease at which a hacker could compromise the nations power infrastructure.
RedHerring

Related Links:
http://www.redherring.com/Article.aspx?a=12275&hed=U.S.+Feds+Target+Hackers&sector=Industries&subsector=SecurityAndDefense

New Vulnerabilities Tested in SecureScout

- **15215 Cumulative Security Update for Internet Explorer (MS05-025/883939) (Remote File Checking)**

A remote code execution vulnerability exists in Internet Explorer because of the way that it handles PNG images. An attacker could exploit the vulnerability by constructing a malicious PNG image that 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.

An information disclosure vulnerability exists in Internet Explorer because of the way that it handles certain requests to display XML content. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially lead to information disclosure if a user visited a malicious Web site or viewed a malicious e-mail message. An attacker who successfully exploited this vulnerability could read XML data from another Internet Explorer domain. 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/MS05-025.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1211
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0648

CVE Reference: CAN-2005-1211, CAN-2002-0648

❖ 15216 Vulnerability in HTML Help Could Allow Remote Code Execution (MS05-026/896358) (Remote File Checking)

A remote code execution vulnerability exists in HTML Help 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:

http://www.microsoft.com/technet/security/bulletin/MS05-026.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1208

CVE Reference: CAN-2005-1208

❖ 15217 Vulnerability in Server Message Block Could Allow Remote Code Execution (MS05-027/896422) (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.

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

References:

http://www.microsoft.com/technet/security/bulletin/MS05-027.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1206

CVE Reference: CAN-2005-1206

❖ 15218 Vulnerability in Web Client Service Could Allow Remote Code Execution (MS05-028/896426) (Remote File Checking)

A remote code execution vulnerability exists in the way that Windows processes Web Client requests that could allow an attacker who successfully exploited this vulnerable to 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/MS05-028.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1207

CVE Reference: CAN-2005-1207

❖ 15219 Vulnerability in Outlook Web Access for Exchange Server 5.5 Could Allow Cross-Site Scripting Attacks (MS05-029/895179) (Remote File Checking)

This is a cross-site scripting vulnerability. 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 Outlook Web Access server that was accessible to the individual user.

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

References:

http://www.microsoft.com/technet/security/Bulletin/MS05-029.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0563

CVE Reference: CAN-2005-0563

❖ 15220 Cumulative Security Update in Outlook Express (MS05-030/897715) (Remote File Checking)

A remote code execution vulnerability exists in Outlook Express when it is used as a newsgroup reader. An attacker could exploit the vulnerability by constructing a malicious newsgroup server that could that potentially allow remote code execution if a user queried the server for news. An attacker who successfully exploited this vulnerability could take complete control of an affected system. 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/MS05-030.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1213

CVE Reference: CAN-2005-1213

❖ 15221 Vulnerability in Step-by-Step Interactive Training Could Allow Remote Code Execution (MS05-031/898458) (Remote File Checking)

A remote code execution vulnerability exists in Step-by-Step Interactive Training because of the way that Step-by-Step Interactive Training handles bookmark link files. An attacker could exploit the vulnerability by constructing a malicious bookmark link file that could potentially allow remote code execution if a user visited a malicious Web site or opened a malicious attachment that was provided in an 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.

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

References:

http://www.microsoft.com/technet/security/bulletin/MS05-031.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1212

CVE Reference: CAN-2005-1212

❖ 15222 Vulnerability in Microsoft Agent Could Allow Spoofing (MS05-032/890046) (Remote File Checking)

This is a spoofing vulnerability that exists in the affected products and that could enable an attacker to spoof trusted Internet content. Users could believe that they are accessing trusted Internet content. However, they are accessing malicious Internet content such as a malicious Web site. An attacker would first have to persuade a user to visit the attacker's site to attempt to exploit this vulnerability.

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

References:

http://www.microsoft.com/technet/security/bulletin/MS05-032.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1214

CVE Reference: CAN-2005-1214

❖ 15223 Vulnerability in Telnet Client Could Allow Information Disclosure (MS05-033/896428) (Remote File Checking)

An attacker who successfully exploited this information disclosure vulnerability could remotely read the session variables for users who have open connections to a malicious telnet server.

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

References:

http://www.microsoft.com/technet/security/bulletin/MS05-033.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1205

CVE Reference: CAN-2005-1205

- **15224 Cumulative Security Update for ISA Server 2000 (MS05-034/899753) (Remote File Checking)**

A vulnerability exists in ISA Server 2000 because of the way that it handles malformed HTTP requests. An attacker could exploit the vulnerability by constructing a malicious HTTP request that could potentially allow an attacker to poison the cache of the affected ISA server. As a result, the attacker could either bypass content restrictions and access content that they would normally not have access to or they could cause users to be directed to unexpected content. Additionally, an attacker could use this in combination with a separate Cross Site Scripting vulnerability to obtain sensitive information such as logon credentials.

An elevation of privilege vulnerability exists in ISA Server 2000 that could allow an attacker who successfully exploited this vulnerability to create a NetBIOS connection with an ISA Server by utilizing the NetBIOS (all) predefined packet filter. The attacker would be limited to services that use the NetBIOS protocol running on the affected ISA Server.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Medium** Risk: **Gain Root**

References:

http://www.microsoft.com/technet/security/Bulletin/MS05-034.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1215
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1216

CVE Reference: CAN-2005-1215, CAN-2005-1216

New Vulnerabilities found this Week

- **SquirrelMail Cross-Site Scripting Vulnerabilities**
  "Cross-site scripting attacks"

  Several vulnerabilities have been reported in SquirrelMail, which can be exploited by malicious people to conduct cross-site scripting attacks.

The vulnerabilities are caused due to unspecified errors and can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site via either URL manipulation or by sending a specially crafted email to a user.

The vulnerabilities have been reported in versions 1.4.0 through 1.4.4. Prior versions may also be affected.

References:
http://www.squirrelmail.org/security/issue/2005-06-15

- **Symantec pcAnywhere Privilege Escalation Vulnerability**

"Gain escalated privileges"

A vulnerability has been reported in pcAnywhere, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to a design error making it possible for a non-privileged, local user to gain SYSTEM privileges by manipulating the "Caller Properties" feature to run arbitrary commands when the system is restarted.

Successful exploitation requires that the program has been configured to run as a service ("Launch with Windows" setting enabled).

References:
http://securityresponse.symantec.com/avcenter/security/Content/2005.06.10.html

- **Macromedia Products Privilege Escalation Vulnerability**

"Gain escalated privileges"

A vulnerability has been reported in various Macromedia products, which potentially can be exploited by malicious, local users to gain escalated privileges.

The problem is that the configuration for the Macromedia Licensing Service has improper permissions and can be modified by arbitrary users. This may be exploited to execute arbitrary code with escalated privileges.

References:
http://www.macromedia.com/devnet/security/security_zone/mpsb05-04.html

- **Novell iManager OpenSSL Denial of Service Vulnerability**

"Denial of Service"

Dennis Rand has reported a vulnerability in Novell iManager, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to a NULL pointer dereference error in the included version of OpenSSL within the ASN.1 parsing code. This can be exploited via a specially crafted packet to crash the web service.

The vulnerability has been reported in version 2.0.2. Other versions may also be affected.

References:
http://cirt.dk/advisories/cirt-32-advisory.pdf

❖ **Novell eDirectory MS-DOS Device Name Denial of Service**

"Denial of Service"

Dennis Rand has reported a vulnerability in Novell eDirectory, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to a NULL pointer dereference error when handling HTTP requests for reserved MS-DOS device names and can be exploited to crash the NDS service.

The vulnerability has been reported in version 8.7.3 for Windows. Prior versions may also be affected.

References:
http://cirt.dk/advisories/cirt-33-advisory.pdf

❖ **Microsoft Outlook Web Access Script Insertion Vulnerability**

"Script insertion attacks"

Gaël Delalleau has reported a vulnerability in Microsoft Exchange Server, which can be exploited by malicious people to conduct script insertion attacks.

The vulnerability is caused due to insufficient validation of HTML messages in Outlook Web Access. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site when a specially crafted message is viewed.

References:
http://www.microsoft.com/technet/security/bulletin/ms05-029.mspx

❖ **Microsoft Windows Web Client Service Vulnerability**

"Gain escalated privileges"

Mark Litchfield has reported a vulnerability in Microsoft Windows, which can be exploited by malicious, local users to gain escalated privileges and by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the handling of messages. This can be exploited by tricking a user into connecting to a malicious WebDAV service and sending specially crafted messages via WebDAV to the Web Client Service.

References:
http://www.microsoft.com/technet/security/Bulletin/MS05-028.mspx

- **Microsoft Outlook Express News Reading Buffer Overflow**

"Buffer overflow"

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

The vulnerability is caused due to a boundary error within the parsing of NNTP responses when using Outlook Express as a newsgroup reader. This can be exploited to cause a buffer overflow via a malicious newsgroup server.

Successful exploitation requires that a user queries a malicious newsgroup server for news.

References:
http://www.microsoft.com/technet/security/bulletin/ms05-030.mspx

- **Microsoft ISA Server Two Vulnerabilities**

"Manipulate contents in the web cache or bypass certain security restrictions"

Two vulnerabilities have been reported in Microsoft ISA Server 2000, which can be exploited by malicious people to manipulate contents in the web cache or bypass certain security restrictions.

1) An error in the handling of malformed HTTP requests containing multiple "Content-Length" headers can be exploited to poison the web cache of the ISA server.

Successful exploitation may allow bypassing of content restrictions or cause users' requests to be redirected, but requires that the ISA server has been configured to publish a web server or proxy web content.

2) An error when validating NetBIOS connections can be exploited by malicious people to create a NetBIOS connection with the ISA server via the NetBIOS (all) predefined packet filter.

Successful exploitation requires that the NetBIOS (all) predefined packet filter has been enabled to allow access to local services using the NetBIOS protocol.

A security issue has also been reintroduced by a previous patch, which may result in Basic Credentials being sent over an external HTTP connection even though SSL is required.

References:
http://www.microsoft.com/technet/security/bulletin/ms05-034.mspx

- **Microsoft Telnet Client Information Disclosure Weakness**

"Gain knowledge of various information"

Gaël Delalleau has reported a weakness in Microsoft Windows, which can be exploited by malicious people to gain knowledge of various information.

The problem is caused due to a design error in the Telnet client when handling the NEW-ENVIRON
command. This can be exploited to gain knowledge of the session variables for a user, who has an open connection to a malicious Telnet server.

Successful exploitation requires that a user e.g. visits a malicious web site or is tricked into clicking a specially crafted link.

References:
http://www.microsoft.com/technet/security/bulletin/ms05-033.mspx

- **Microsoft Agent Trusted Internet Content Spoofing Vulnerability**

"Trick a user into installing a malicious program"

A vulnerability has been reported in Microsoft Windows, which can be exploited by malicious people to spoof certain information and potentially trick a user into installing a malicious program.

The vulnerability is caused due to an error in Microsoft Agent making it possible to spoof trusted Internet content (e.g. hide various security prompts by a Microsoft Agent character). This can be exploited to trick a user into believing that they are looking at trusted content when actually visiting a malicious web site.

Successful exploitation requires that a user visits a malicious web site.

References:
http://www.microsoft.com/technet/security/bulletin/ms05-032.mspx

❖ **Microsoft Windows HTML Help Input Validation Vulnerability**

"Integer overflow"

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

The vulnerability is caused due to an integer overflow within HTML Help and can be exploited to cause a heap-based buffer overflow via a specially crafted Help (.chm) file with a very high value in a size field.

Successful exploitation allows execution of arbitrary code.

References:
http://www.microsoft.com/technet/security/Bulletin/MS05-026.mspx

❖ **Microsoft Windows Step-by-Step Interactive Training Vulnerability**

"Boundary error"

iDEFENSE Labs has reported a vulnerability in Microsoft Windows, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the Step-by-Step Interactive Training component when handling bookmark link files. This can be exploited to cause a stack-based buffer overflow via a specially crafted bookmark link file containing an overly long string in the "User" field.

Successful exploitation requires that the user e.g. visits a malicious web site or opens a malicious attachment.

References:
http://www.microsoft.com/technet/security/bulletin/ms05-031.mspx

❖ **Internet Explorer Two Vulnerabilities**

"Disclose sensitive information"

Two vulnerabilities have been reported in Microsoft Internet Explorer, which can be exploited by malicious people to disclose sensitive information and compromise a users system.

1) The vulnerability is caused due to a boundary error in the PNG rendering engine. This can be exploited to cause a buffer overflow by tricking a user into visiting a malicious web site or view a malicious email containing a specially crafted PNG image.

Successful exploitation allows execution of arbitrary code with the

privileges of the user running Internet Explorer or another program using the PNG rendering engine.

2) The vulnerability is caused due to an error in the verification of redirects from XML resources. This can be exploited by tricking a user into visiting a malicious web site.

Successful exploitation allows exposure of information from remote resources and local files.

Other potentially security related issues have also been addressed by this bulletin.

References:
http://www.microsoft.com/technet/security/Bulletin/MS05-025.mspx

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