netVigilance

ScoutNews Team **15 October 2004**
Issue #42

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

This years SANS/FBI Top 20 was released this week – basically the same old thing, we are more and more vulnerable the same places.
Major phising combined with Trojans is going on at the moment and the publi9c is biting the bate of celebrities like Michael Jackson, David Beckham and the likes.
The weakest link is still the human one.

Enjoy reading

Top Security News Stories this Week

- **Sophos warns internet users of Michael Jackson home movies Trojan horse**

  Experts at Sophos have warned computer users that a file posing as a home movie of popstar Michael Jackson is in fact infected by a malicious Trojan horse. Thousands of sick messages posted to internet newsgroups last night encourage computer users to download a file supposedly containing pictures of Jackson abusing a young boy. In reality, no such photographs are present but the file can open computers up to attack from hackers.

http://www.sophos.com/virusinfo/articles/jackson.html
Sophos

- **Fake Beckham Pix Flood the Net in New Virus Scare**

  Virus writers are attempting to take over computer users' PCs by enticing them to click on a malicious program masquerading as lurid photos of England soccer captain David Beckham, a British security firm warned. According to Sophos Plc., thousands of messages have been posted to Internet message boards in the past week claiming the married soccer star has been photographed with a Spanish prostitute.
  The message instructs the curious to click on a Web link to see the revealing snapshots. But clicking the link will download a program known as a "Trojan horse" -- so named for its ability to sneak onto a PC and take control of the machine.

http://story.news.yahoo.com/news?tmpl=story&ncid=1212&e=10&u=/nm/20041014/wr_nm/tech_internet_beckham_dc&sid=95573503
Reuters

- **SANS Top 20 Vulnerabilities**

  SANS released its annual Top 20 list of Internet security vulnerabilities. According to SANS the list compiled by consensus of contributors from "government agencies in the UK, US, and Singapore; the leading security software vendors and consulting firms; the top university-based security programs; many other user organizations; and the SANS Institute. "

  For Windows, the SANS list suggests that the most vulnerable areas are Web servers & Web services, the Workstation service, RAS, Microsoft SQL Server, Windows authentication, Web browsers, file sharing applications, LSAS exposures, mail clients, and instant messaging. Not much has changed, eh?

  The top 20 vulnerabilities for Unix and Linux platforms are BIND DNS, Web servers, authentication, version control systems, mail transport services, SNMP, Open Secure Sockets Layer (SSL), misconfiguration of NIS/NFS, databases, and the kernel itself.

  You can learn about the specifics of these areas of vulnerability by reading the Top 20 list at the SANS Web site.

http://www.winnetmag.com/Windows/Article/ArticleID/44214/44214.html

Mark Joseph Edwards

New Vulnerabilities Tested in SecureScout

- **14471 Vulnerability in Microsoft Excel Could Allow Remote Code Execution (MS04-033/886836) (Remote File Checking)**

  A remote code execution vulnerability exists in Microsoft Excel.

  If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

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

CVE Links: CAN-2004-0846

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-033.mspx

- **14660 Vulnerability in RPC Runtime Library Could Allow Information Disclosure and Denial of Service (MS04-029/873350) (Remote File Checking)**

  An attacker who successfully exploited the vulnerability could cause the affected system to stop responding or could potentially read portions of active memory content.

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

CVE Links: CAN-2004-0569

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-029.mspx

- **14661 Vulnerability in WebDAV XML Message Handler Could Lead to a**

Denial of Service (MS04-030/824151) (Remote File Checking)

An attacker who successfully exploited this vulnerability could cause WebDAV to consume all available memory and CPU time on an affected server. This behavior could cause a denial of service. The IIS service would have to be restarted to restore functionality.

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

CVE Links: CAN-2003-0718

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-030.mspx

- **14662 Vulnerability in NetDDE Could Allow Remote Code Execution (MS04-031/841533) (Remote File Checking)**

A remote code execution vulnerability exists in the Network Dynamic Data Exchange (NetDDE) services because of an unchecked buffer.

An attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. However, the NetDDE services are not started by default and would have to be manually started, or started by an application that requires NetDDE, for an attacker to attempt to remotely exploit this vulnerability.

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

CVE Link: CAN-2004-0206

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-031.mspx

- **14663 Security Update for Microsoft Windows (MS04-032/840987) (Remote File Checking)**

An attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges.

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

CVE Link: CAN-2004-0207 & CAN-2004-0208 & CAN-2004-0209 & CAN-2004-0211

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-032.mspx

- **14664 Vulnerability in Compressed (zipped) Folders Could Allow Remote Code Execution (MS04-034/873376) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Windows processes Compressed (zipped) Folders.

If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges. However, user interaction is required to exploit this vulnerability.

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

CVE Link: CAN-2004-0575

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-034.mspx

- **15366 Vulnerability in SMTP Could Allow Remote Code Execution (MS04-035/885881) (Remote File Checking)**

  A remote code execution vulnerability exists in the Simple Mail Transfer Protocol (SMTP) component that is provided as part of the affected software.
  An attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges.

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

CVE Link: CAN-2004-0840

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-035.mspx

- **15399 Vulnerability in NNTP Could Allow Remote Code Execution (MS04-036/883935) (Remote File Checking)**

  A remote code execution vulnerability exists within the Network News Transfer Protocol (NNTP) component of the affected operating systems. This vulnerability could potentially affect systems that do not use NNTP. This is because some programs that are listed in the affected software section require that the NNTP component be enabled before you can install them.
  An attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges.

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

CVE Link: CAN-2004-0574

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-036.mspx

- **15414 Vulnerability in SMTP Could Allow Remote Code Execution (MS04-035/885881) (SMTP Check)**

  A remote code execution vulnerability exists in the Simple Mail Transfer Protocol (SMTP) component that is provided as part of the affected software.
  An attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges.

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

CVE Link: CAN-2004-0840

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-035.mspx

- **15415 Vulnerability in NNTP Could Allow Remote Code Execution (MS04-036/883935) (NNTP Check)**

A remote code execution vulnerability exists within the Network News Transfer Protocol (NNTP) component of the affected operating systems. This vulnerability could potentially affect systems that do not use NNTP. This is because some programs that are listed in the affected software section require that the NNTP component be enabled before you can install them.
An attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges.

Test Case Impact: **Gather Info** Vulnerability Impact: **Remote3 Code Execution** Risk: **High**

CVE Link: CAN-2004-0574

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-036.mspx

New Vulnerabilities found this Week

- **MediaWiki Multiple Vulnerabilities**

"Script insertion, cross-site scripting, and SQL injection attacks"
Multiple vulnerabilities have been reported in MediaWiki, which can be exploited by malicious people to conduct script insertion, cross-site scripting, and SQL injection attacks.
1) Input passed in UnicodeConverter extension and "raw" page view is not properly sanitised before being used. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site when the malicious user data is viewed.
2) Input passed to "SpecialIpblocklist", "SpecialEmailuser", "SpecialMaintenance", and "ImagePage" isn't properly sanitised 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 a vulnerable site.
3) MediaWiki fails to verify input passed to "SpecialMaintenance" properly, before it is used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.
The vulnerabilities have been reported in version 1.3.5. Other versions may also be affected.

References:
http://sourceforge.net/project/shownotes.php?release_id=275099

- **ShixxNOTE Font File Handling Buffer Overflow Vulnerability**

"Buffer overflow"
Luigi Auriemma has discovered a vulnerability in ShixxNOTE, which can be exploited by malicious people to compromise a vulnerable system.
The vulnerability is caused due to boundary errors in the handling of font fields. This can

be exploited to cause a buffer overflow by sending a specially crafted message with an overly long font field.
Successful exploitation can lead to execution of arbitrary code.
The vulnerability has been confirmed on version 6.net (build 117). Other versions may also be affected.

References:
http://aluigi.altervista.org/adv/shixxbof-adv.txt

- **LibTIFF Multiple Image Decoder Parsing Vulnerabilities**

"Heap-based buffer overflows"
Multiple vulnerabilities have been reported in LibTIFF, which potentially can be exploited by malicious people to compromise a user's system.
1) Boundary errors within the RLE decoding in "tif_next.c", "tif_thunder.c", and "tif_luv.c" can be exploited to cause heap-based buffer overflows. This can be exploited with a specially crafted TIFF image file to execute arbitrary code via an application linked to the vulnerable library.
2) Some unspecified integer overflows may potentially allow arbitrary code execution on a user's system.
The vulnerabilities have been reported in version 3.6.1. Other versions may also be affected.

References:
http://scary.beasts.org/security/CESA-2004-006.txt

- **phpMyAdmin Unspecified Arbitrary Command Execution Vulnerability**

"Execute arbitrary commands"
A vulnerability has been reported in phpMyAdmin, which potentially can be exploited by malicious people to compromise a vulnerable system.
The vulnerability is caused due to a problem in the MIME-based transformation system with "external" transformations. This can be exploited to execute arbitrary commands.
Successful exploitation requires that PHP's safe mode is disabled.

References:
http://www.phpmyadmin.net/home_page/

- **ocPortal "index.php" Arbitrary File Inclusion Vulnerability**

"Include arbitrary files"
Exoduks has reported a vulnerability in ocPortal, which can be exploited by malicious people to compromise a vulnerable system.
Input passed to the "req_path" parameter in "index.php" is not properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources.
The vulnerability has been reported in version 1.03 and prior.

References:
http://ocportal.com/index.php?page=download

- **Microsoft Windows / Office / Exchange Multiple vulnerabilities**

Vulnerability in RPC Runtime Library Could Allow Information Disclosure and Denial of Service (MS04-029)
Vulnerability in WebDAV XML Message Handler Could Lead to a Denial of Service (MS04-030)
Vulnerability in NetDDE Could Allow Remote Code Execution (MS04-031)
Security Update for Microsoft Windows (MS04-032)
Vulnerability in Microsoft Excel Could Allow Remote Code Execution (MS04-033)
Vulnerability in Compressed (zipped) Folders Could Allow Remote Code Execution (MS04-034)
Vulnerability in SMTP Could Allow Remote Code Execution (MS04-035)
Vulnerability in NNTP Could Allow Remote Code Execution (MS04-036)
Vulnerability in Windows Shell Could Allow Remote Code Execution (MS04-037)
Cumulative Security Update for Internet Explorer (MS04-038)

References:
http://www.microsoft.com/technet/security/bulletin/MS04-029.mspx
http://www.microsoft.com/technet/security/bulletin/MS04-030.mspx
http://www.microsoft.com/technet/security/bulletin/MS04-031.mspx
http://www.microsoft.com/technet/security/bulletin/MS04-032.mspx
http://www.microsoft.com/technet/security/bulletin/MS04-033.mspx
http://www.microsoft.com/technet/security/bulletin/MS04-034.mspx
http://www.microsoft.com/technet/security/bulletin/MS04-035.mspx
http://www.microsoft.com/technet/security/bulletin/MS04-036.mspx
http://www.microsoft.com/technet/security/bulletin/MS04-037.mspx
http://www.microsoft.com/technet/security/bulletin/MS04-038.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