netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 33

August 18, 2006

Table of Contents

Product Focus

Sasser Worm Scanner – The Sasser Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Microsoft SSL Vulnerability (MS04-011) that used by the Sasser Worm to infect machines.

This Week in Review

Banks are increasing online banking security. SW makers: It is time to look into how flaws are handled. Blackberry a rising threat? International group formed to boost government's understanding of privacy and ID issues in modern technology.

Enjoy reading & Stay safe

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

Top Security News Stories this Week

- **Taking IT security to the next level**

Many banks have been increasing the security of their online services over the past year. By offering customers smartcard readers or security tokens, they have been able to roll out a second level of security.

The move highlights how businesses' faith in passwords is declining - if they are not lost, they can be stolen,...

... and if they aren't stolen, they can be easily shared.

Two-factor authentication raises the security bar, introducing another level of authentication for system access. Generally, two-factor authentication uses something a user knows (a password or Pin) along with something they have (a security token), making impersonation more difficult.

It has been used to authenticate both employees and customers, but it has limitations. With corporate governance regulations such as Sarbanes-Oxley requiring stronger authentication as part of an overall hardening of security, more large companies are likely to investigate two-factor authentication, but small to mid-range companies have a habit of lax security practice. Passwords are regularly exchanged and written down.

Computerweekly.com

Full Story :
http://www.computerweekly.com/Home/Articles/2006/08/15/217595/Taking+IT+security+to+the+next+level.htm

❖ Flaw finders to software makers: It's payback time

Bug hunters are turning the tables on software makers in the debate over reporting flaws.

In recent years, software companies have hammered out rules with researchers on disclosure, which cover how and when vulnerabilities are made public. Now flaw finders want something in return: more information from software providers on what they are doing to tackle the holes the researchers have reported.

"We have gone from the old 'full disclosure' to 'responsible disclosure' debate, to a debate over 'The vendor has the information--what does it do with it?'" said Steven Lipner, senior director for security engineering strategy at Microsoft.

ZDNet

Full Story :
http://news.zdnet.com/2100-1009_22-6106593.html

❖ BlackBerry gateway for attacks

A CALIFORNIA computer security specialist has released software to show hackers can attack networks through BlackBerry handheld devices.

Jesse D'Aguanno of Praetorian Global made a "BlackBerry Attack Toolkit" demonstration available for download at the company's website along with "BBProxy" software that exploits the vulnerability.

"The premise is the BlackBerry device that everyone carries around in their holsters is actually a computer constantly connected to your network," Mr D'Aguanno said.

AustralianIT

Full Story :
http://australianit.news.com.au/articles/0,7204,20133450%5E15321%5E%5Enbv%5E15306,0

0.html

- **New e-gov group helps with digital IDs**

A new e-government group has been formed by the Liberty Alliance to help governments adopt open standards, and understand privacy and ID issues surrounding modern technology.
The Liberty Alliance is an international consortium of companies and organisations that focuses on the technical and policy issues surrounding digital identities. So far, it has supported a range of protocols and standards that, among other things, allow users to move easily from one website to another without having enter a password each time.
The eGovernment Group includes representatives from Denmark, Finland, France, Korea, New Zealand, the UK and the US. The group is chaired by Colin Wallis, of the New Zealand Government's State Services Commission.

Techworld

Full Story :
http://www.techworld.com/security/news/index.cfm?newsID=6663&pagtype=samechan

New Vulnerabilities Tested in SecureScout

- **16292 Oracle Vulnerability in Server Service Could Allow Remote Code Execution (MS06-040/921883) (Remote File Checking)**

There is a remote code execution vulnerability in Server 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: **Attack** Risk: **High**

References:

Original advisory:
MS:MS06-040
URL:http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx

Other references:
CERT:TA06-220A
URL:http://www.us-cert.gov/cas/techalerts/TA06-220A.html
CERT-VN:VU#650769
URL:http://www.kb.cert.org/vuls/id/650769
FRSIRT:ADV-2006-3210
URL:http://www.frsirt.com/english/advisories/2006/3210
SECUNIA:21388
URL:http://secunia.com/advisories/21388

CVE Reference: CVE-2006-3439

❖ 16293 Oracle Vulnerabilities in DNS Resolution Could Allow Remote Code Execution (MS06-041/920683) (Remote File Checking)

Vulnerabilities in DNS Resolution Could Allow Remote Code Execution (MS06-041/920683) (Remote File Checking)

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

References:

Original advisory:
* MS:MS06-041
* URL:http://www.microsoft.com/technet/security/bulletin/ms06-041.mspx

Other references:
* CERT:TA06-220A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-220A.html
* CERT-VN:VU#908276
* URL:http://www.kb.cert.org/vuls/id/908276
* CERT-VN:VU#794580
* URL:http://www.kb.cert.org/vuls/id/794580

CVE Reference: CVE-2006-3440

❖ 16294 Oracle Cumulative Security Update for Internet Explorer (MS06-042/918899) (Remote File Checking)

An information disclosure vulnerability exists in Internet Explorer in the way that a redirect is handled. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow for information disclosure if a user viewed the Web page. An attacker who successfully exploited this vulnerability could read file data from a Web page in another Internet Explorer domain. This other Web page must use gzip encoding or some other compression type supported by Internet Explorer for any information disclosure to occur. This other Web page must also be cached on the client side for a successful exploit.

A remote code execution vulnerability exists in the way Internet Explorer interprets HTML with certain layout positioning combinations. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user viewed the Web page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A remote code execution vulnerability exists in the way Internet Explorer handles chained Cascading Style Sheets (CSS). An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user viewed the Web page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A remote code execution vulnerability exists in the way Internet Explorer interprets HTML with certain layout combinations. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code

execution if a user viewed the Web page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A remote code execution vulnerability exists in the way Internet Explorer instantiates COM objects that are not intended to be instantiated in Internet Explorer. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user viewed the Web page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A remote code execution and information disclosure vulnerability exists in Internet Explorer in the way that a redirect is handled. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow for information disclosure if a user viewed the Web page. An attacker who successfully exploited this vulnerability could read file data from a Web page in another Internet Explorer domain.

On Windows 2000 Service Pack 4 and Windows XP Service Pack 1 an attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user viewed the Web page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

An information disclosure vulnerability exists in Internet Explorer where script can be persisted across navigations and used to gain access to the location of a Window in another domain or Internet Explorer zone. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow for information disclosure if a user viewed the Web page. An attacker who successfully exploited this vulnerability could gain access to the Window location of a Web page in another domain or Internet Explorer zone.

An elevation of privilege vulnerability exists in the way Internet Explorer handles specially crafted FTP links that contain line feeds. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow the attacker to issue FTP server commands if a user clicked on an FTP link. An attacker who successfully exploited this vulnerability could issue server commands as the user to servers.

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

References:

Original advisory:
* MS:MS06-042
* URL:http://www.microsoft.com/technet/security/bulletin/ms06-042.mspx

CVE Reference: CVE-2006-3280
CVE-2006-3450
CVE-2006-3451
CVE-2006-3637
CVE-2006-3638
CVE-2006-3639
CVE-2006-3640
CVE-2004-1166

❖ 16295 Vulnerability in Microsoft Windows Could Allow Remote Code Execution (MS06-043/920214) (Remote File Checking)

There is a remote code execution vulnerability in Windows that results from incorrect parsing of the MHTML protocol. An attacker could exploit the vulnerability by constructing a specially crafted Web page or HTML e-mail that could potentially lead to remote code execution if a user visited a specially crafted Web site or clicked a link in a specially crafted e-mail message.

If a user were logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.
Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **High**

References:

Original advisory:
* MS:MS06-043
* URL:http://www.microsoft.com/technet/security/Bulletin/MS06-043.mspx

Other references:
* BUGTRAQ:20060531 Internet explorer Vulnerbility
* URL:http://www.securityfocus.com/archive/1/archive/1/435492/100/0/threaded
* BUGTRAQ:20060601 RE: Internet explorer Vulnerbility
* URL:http://www.securityfocus.com/archive/1/435616/100/0/threaded
* BUGTRAQ:20060601 Re: Internet explorer Vulnerbility
* URL:http://www.securityfocus.com/archive/1/435609/100/0/threaded
* CERT:TA06-220A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-220A.html
* CERT-VN:VU#891204
* URL:http://www.kb.cert.org/vuls/id/891204
* BID:18198
* URL:http://www.securityfocus.com/bid/18198
* FRSIRT:ADV-2006-2088
* URL:http://www.frsirt.com/english/advisories/2006/2088
* SECUNIA:20384
* URL:http://secunia.com/advisories/20384

CVE Reference: CVE-2006-2766

❖ 16296 Vulnerability in Microsoft Management Console Could Allow Remote Code Execution (MS06-044/917008) (Remote File Checking)

There is a remote code execution vulnerability in Windows Management Console 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: **Attack** Risk: **High**

References:

Original advisory:
* MS:MS06-044
* URL:http://www.microsoft.com/technet/security/Bulletin/MS06-044.mspx

Other references:
* CERT:TA06-220A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-220A.html
* CERT-VN:VU#927548
* URL:http://www.kb.cert.org/vuls/id/927548

CVE Reference: CVE-2006-3643

❖ 16297 Vulnerability in Windows Explorer Could Allow Remote Code Execution (MS06-045/921398) (Remote File Checking)

A remote code execution vulnerability exists in Windows Explorer because of the way that Windows Explorer handles Drag and Drop events. An attacker could exploit the vulnerability by constructing a malicious Web page that 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. User interaction is required to exploit this vulnerability

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

References:

Original advisory:
* MS:MS06-045
* URL:http://www.microsoft.com/technet/security/Bulletin/MS06-045.mspx

Other references:
* FULLDISC:20060627 IE_ONE_MINOR_ONE_MAJOR
* URL:http://lists.grok.org.uk/pipermail/full-disclosure/2006-June/047398.html
* MISC: http://lists.grok.org.uk/pipermail/full-disclosure/attachments/20060627/3d930eda/PLEBO-2006.06.16-IE_ONE_MINOR_ONE_MAJOR.obj
* CERT:TA06-220A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-220A.html
* CERT-VN:VU#655100
* URL:http://www.kb.cert.org/vuls/id/655100
* BID:19389
* URL:http://www.securityfocus.com/bid/19389
* FRSIRT:ADV-2006-2553
* URL:http://www.frsirt.com/english/advisories/2006/2553

* SECTRACK:1016388
* URL:http://securitytracker.com/id?1016388
* SECUNIA:20825
* URL:http://secunia.com/advisories/20825
* XF:ie-hta-fileshare-command-execution(27456)
* URL:http://xforce.iss.net/xforce/xfdb/27456

CVE Reference: CVE-2006-3281

❖ 16298 Oracle Vulnerability in HTML Help Could Allow Remote Code Execution (MS06-046/922616) (Remote File Checking)

A vulnerability exists in the HTML Help ActiveX control that could allow 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: **Attack** Risk: **High**

References:

Original advisory:
* MS:MS06-046
* URL:http://www.microsoft.com/technet/security/Bulletin/MS06-046.mspx

Other references:
* MISC: http://browserfun.blogspot.com/2006/07/mobb-2-internethhctrl-image-property.html
* CERT:TA06-220A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-220A.html
* CERT-VN:VU#159220
* URL:http://www.kb.cert.org/vuls/id/159220
* BID:18769
* URL:http://www.securityfocus.com/bid/18769
* FRSIRT:ADV-2006-2634
* URL:http://www.frsirt.com/english/advisories/2006/2634
* FRSIRT:ADV-2006-2635
* URL:http://www.frsirt.com/english/advisories/2006/2635
* OSVDB:26835
* URL:http://www.osvdb.org/26835
* SECTRACK:1016434
* URL:http://securitytracker.com/id?1016434
* SECUNIA:20906
* URL:http://secunia.com/advisories/20906
* XF:ie-hhctrl-bo(27573)
* URL:http://xforce.iss.net/xforce/xfdb/27573

CVE Reference: CVE-2006-3357

❖ 16299 Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution (MS06-047/921645) (Remote File

Checking)

A remote code execution vulnerability exists in the way that Visual Basic for Applications (VBA) checks the document properties that a host application passes to it when opening a document. This vulnerability could allow an attacker who successfully exploited the vulnerability to take complete control of the affected system.

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

References:

Original advisory:
MS:MS06-047
URL:http://www.microsoft.com/technet/security/Bulletin/MS06-047.mspx

Other references:
CERT:TA06-220A
URL:http://www.us-cert.gov/cas/techalerts/TA06-220A.html
CERT-VN:VU#159484
URL:http://www.kb.cert.org/vuls/id/159484

CVE Reference: CVE-2006-3649

❖ **16300 Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS06-048/922968) (Remote File Checking)**

A remote code execution vulnerability exists in PowerPoint and could be exploited when a file containing a malformed shape container is parsed by PowerPoint. Such a file might be included in an e-mail attachment or hosted on a malicious web site. An attacker could exploit the vulnerability by constructing a specially crafted PowerPoint file that could allow remote code execution.

A remote code execution vulnerability exists in PowerPoint and could be exploited when a file containing a malformed record is parsed by PowerPoint. Such a file might be included in an e-mail attachment or hosted on a malicious web site. An attacker could exploit the vulnerability by constructing a specially crafted PowerPoint file that could allow remote code execution.

If a user were logged on with administrative user rights, an attacker who successfully exploited one of these vulnerabilities could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

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

References:

Original advisory:
* MS:MS06-048

* URL:http://www.microsoft.com/technet/security/Bulletin/MS06-048.mspx

Other references:
* BUGTRAQ:20060714 Microsoft PowerPoint 0-day Vulnerability FAQ document written
* URL:http://www.securityfocus.com/archive/1/archive/1/440137/100/0/threaded
* BUGTRAQ:20060716 Several updates in MS PowerPoint 0-day Vulnerability FAQ at SecuriTeam Blogs
* URL:http://www.securityfocus.com/archive/1/archive/1/440255/100/0/threaded
* BUGTRAQ:20060718 New PowerPoint Trojan installs itself as LSP
* URL:http://www.securityfocus.com/archive/1/archive/1/440532/100/0/threaded
* MISC:
http://securityresponse.symantec.com/avcenter/venc/data/trojan.ppdropper.b.html
* MISC: http://isc.sans.org/diary.php?storyid=1484
* MISC: http://blogs.securiteam.com/?p=508
* CERT-VN:VU#936945
* URL:http://www.kb.cert.org/vuls/id/936945
* BID:18957
* URL:http://www.securityfocus.com/bid/18957
* FRSIRT:ADV-2006-2795
* URL:http://www.frsirt.com/english/advisories/2006/2795
* SECTRACK:1016496
* URL:http://securitytracker.com/id?1016496
* SECUNIA:21040
* URL:http://secunia.com/advisories/21040
* XF:powerpoint-mso-code-execution(27740)
* URL:http://xforce.iss.net/xforce/xfdb/27740
* XF:powerpoint-mso-code-execution2(27781)
* URL:http://xforce.iss.net/xforce/xfdb/27781
* BUGTRAQ:20060808 Microsoft PowerPoint Malformed Record Memory Corruption
* URL:http://www.securityfocus.com/archive/1/archive/1/442592/100/0/threaded
* MISC: http://secway.org/advisory/AD20060808.txt
* CERT:TA06-220A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-220A.html
* CERT-VN:VU#884252
* URL:http://www.kb.cert.org/vuls/id/884252

CVE Reference: CVE-2006-3590

❖ 16301 Vulnerability in Windows Kernel Could Result in Elevation of Privilege (MS06-049/920958) (Remote File Checking)

There is a privilege elevation vulnerability in Windows 2000 caused by improper validation of system inputs. This vulnerability could allow a logged on user to take complete control of the system.

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

References:

Original advisory:
* MS:MS06-049
* URL:http://www.microsoft.com/technet/security/Bulletin/MS06-049.mspx

Other references:
* BID:19388
* URL:http://www.securityfocus.com/bid/19388

CVE Reference: CVE-2006-3444

New Vulnerabilities found this Week

Avaya Products Integer Overflow and Denial of Service
"Denial of Service"

Avaya has acknowledged two vulnerabilities in the python and gnupg packages included in various Avaya products, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially to compromise a vulnerable system.

The following products are affected:
* Avaya Intuity LX (all versions)
* Avaya Messaging Storage Server (all versions)
* Avaya Message Networking (all versions)

References:
http://support.avaya.com/elmodocs2/security/ASA-2006-159.htm
http://support.avaya.com/elmodocs2/security/ASA-2006-164.htm

Kolab Server ClamAV Buffer Overflow Vulnerability
"Denial of Service"

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

References:
http://kolab.org/security/kolab-vendor-notice-10.txt

Sun Solaris netstat/SNMP queries and ifconfig Race Condition
"Denial of Service"

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

The vulnerability is caused due to a race condition between netstat or SNMP queries and ifconfig, which may lead to a system panic.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102569-1

Novell eDirectory Denial of Service and Password Exposure
"Denial of Service"

A vulnerability and a security issue have been reported in Novell eDirectory, which

potentially can be exploited by malicious, local users to disclose sensitive information and by malicious people to cause a DoS (Denial of Service).

1) An unspecified error may exhaust CPU resources during a Nessus scan.

2) The eMBoxClient.jar iManager prints user passwords in a log file.

NOTE: Other issues, where some may be security related, have also been reported.

References:
http://support.novell.com/cgi-bin/search/searchtid.cgi?/2973826.htm

Apache "mod_alias" URL Validation Canonicalization Vulnerability

"Bypass security restrictions; disclose potentially sensitive information"

Susam Pal has discovered a vulnerability in Apache, which can be exploited by malicious people to bypass certain security restrictions and disclose potentially sensitive information.

The vulnerability is caused due to a canonicalization error in the "mod_alias" module in the handling of case-sensitive alias directive arguments on file systems supporting case-insensitive directory names. This can e.g. be exploited to disclose the source code of applications placed in the "cgi-bin" directory on certain non-default configurations where the ScriptAlias directive references a directory inside the document root by accessing an URL with a capital directory name (e.g. "CGI-BIN").

Example of a vulnerable configuration:
DocumentRoot "[path]/docroot/"
ScriptAlias /cgi-bin/ "/[path]/docroot/cgi-bin"

NOTE: This only affects the Microsoft Windows platform.

The vulnerability has been confirmed in versions 2.0.59 and 2.2.3, and has also been reported in version 2.2.2. Other versions may also be affected.

References:
http://www.frsirt.com/english/advisories/2006/3265

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