netVigilance assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 7

February 15, 2008

Table of Contents

Product Focus

Sapphire Worm Scanner – The Sapphire 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 SQL buffer overflow vulnerability (MS02-039/MS02-061) that the recent Sapphire Worm uses to propagate.

Check out our video section for a number of interviews with Jesper Jurcenoks: www.netvigilance.com/videos

This Week in Review

PCI rules getting better. Happy Valentine's - but be careful out there. Fake dns servers more active. Phone viruses expected but not there yet.

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

❖ Payment Card Industry (PCI) update

PCI looking the wrong way, but rules will help everyone.
Credit card losses to fraud adds up to about $3 Billion per year, depending on who you ask. So we can understand the concern on the part of financial service

> companies and the need for the Payment Card Industry Data Security Standard (PCI DSS, usually referred to as just PCI; official documents here).
> But the huge credit card companies -- Visa, MasterCard, American Express, Discover, and JCB -- haven't done their job well and are forcing new rules on the wrong end of the transaction pipeline. That said, the rules are, for the most part, good security guidelines that businesses should be following anyway. Rarely do we see a bad idea lead to good results.

linuxworld

Full Story :
http://www.linuxworld.com/columnists/2008/021108gaskin.html

❖ Storm clouds Valentine's Day inboxes

The Storm worm is showing no signs of letting up in its Valentine's Day assault.

Researchers from major security firms have uncovered thousands of spam emails spreading the Trojan in the days leading up to 14 February.

The worm has been spreading since January in the form of email greeting cards with subjects as 'You Stay in My Heart' and 'Thinking of U All Day'.

Users are taken to a fake e-card site and asked to download an application called 'valentine.exe'. The executable file is a Trojan which will add the user's computer to the huge Storm botnet.

vnunet

Full Story :
http://www.vnunet.com/vnunet/news/2209625/love-lost-storm-valentine

❖ Use of rogue DNS servers on rise

Fraudulent Web sites increasingly used to launch attacks
SAN FRANCISCO - They're called "servers that lie."

Mendacious machines controlled by hackers that reroute Internet traffic from infected computers to fraudulent Web sites are increasingly being used to launch attacks, according to a paper published this week by researchers with the Georgia Institute of Technology and Google Inc.

The paper estimates roughly 68,000 servers on the Internet are returning malicious Domain Name System results, which means people with compromised computers are sometimes being directed to the wrong Web sites — and often have no idea.

msnbc

Full Story :
http://www.msnbc.msn.com/id/23152055/

❖ Phone viruses to spread as telecom, computer worlds merge, say experts

Viruses and hacking on mobile phones are still rare but attacks are a looming danger as increasing numbers of people access the Internet and download files with their handsets, experts say.

A survey released this week at the industry's Mobile World Congress showed that only 2.1 percent of people had been struck by a virus themselves and only 11.6 percent knew someone who had been affected by one.

The poll by IT security specialist McAfee, based on 2,000 people in Britain, the United States and Japan, showed that 86.3 percent had had no experience of mobile phone viruses.

Yahoo news

Full Story :
http://news.yahoo.com/s/afp/20080213/tc_afp/telecominternetvirus

New Vulnerabilities Tested in SecureScout

❖ 16859 Microsoft Office Execution Jump Vulnerability (MS08-013/947108) (Remote File Checking)

The vulnerability could allow remote code execution if a user opens a specially crafted Microsoft Office document with a malformed object inserted into the document. 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 impacted than users who operate with administrative user rights.

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

References:

* MS: MS08-013
http://www.microsoft.com/technet/security/bulletin/ms08-013.mspx
* CERT: TA08-043C
http://www.us-cert.gov/cas/techalerts/TA08-043C.html
* BID: 27738
http://www.securityfocus.com/bid/27738
* FRSIRT: ADV-2008-0515
http://www.frsirt.com/english/advisories/2008/0515/references
* SECTRACK: 1019375
http://www.securitytracker.com/id?1019375
* SECUNIA: 28909
http://secunia.com/advisories/28909

CVE Reference: CVE-2008-0103

❖ 16858 Word Memory Corruption Vulnerability (MS08-009/947077) (Remote File Checking)

A remote code execution vulnerability exists in the way that Word handles specially crafted Word files. The vulnerability could allow remote code execution if a user opens a specially crafted Word file that includes a malformed value. 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.

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

References:

* MS: MS08-009
http://www.microsoft.com/technet/security/bulletin/ms08-009.mspx
* CERT: TA08-043C
http://www.us-cert.gov/cas/techalerts/TA08-043C.html
* CERT-VN: VU#692417
http://www.kb.cert.org/vuls/id/692417
* BID: 27656
http://www.securityfocus.com/bid/27656
* FRSIRT: ADV-2008-0511
http://www.frsirt.com/english/advisories/2008/0511/references
* SECTRACK: 1019374
http://www.securitytracker.com/id?1019374
* SECUNIA: 28901
http://secunia.com/advisories/28901

CVE Reference: CVE-2008-0109

❖ 16857 Publisher Memory Corruption Vulnerability (MS08-012/947085) (Remote File Checking)

A remote code execution vulnerability exists in the way Microsoft Office Publisher validates memory index values. An attacker could exploit the vulnerability by constructing a specially crafted Publisher (.pub) file. When a user views the .pub file, the vulnerability could allow remote code execution. 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.

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

References:

* MS: MS08-012

http://www.microsoft.com/technet/security/bulletin/ms08-012.mspx
* CERT: TA08-043C
http://www.us-cert.gov/cas/techalerts/TA08-043C.html
* BID: 27740
http://www.securityfocus.com/bid/27740
* FRSIRT: ADV-2008-0514
http://www.frsirt.com/english/advisories/2008/0514/references
* SECTRACK: 1019377
http://www.securitytracker.com/id?1019377
* SECUNIA: 28906
http://secunia.com/advisories/28906

CVE Reference: CVE-2008-0104

❖ 16856 Publisher Invalid Memory Reference Vulnerability (MS08-012/947085) (Remote File Checking)

A remote code execution vulnerability exists in the way Microsoft Office Publisher validates application data when loading Publisher files to memory. An attacker could exploit the vulnerability by constructing a specially crafted Publisher (.pub) file. When a user views the .pub file, the vulnerability could allow remote code execution. 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.

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

References:

* MS: MS08-012
http://www.microsoft.com/technet/security/bulletin/ms08-012.mspx
* CERT: TA08-043C
http://www.us-cert.gov/cas/techalerts/TA08-043C.html
* BID: 27739
http://www.securityfocus.com/bid/27739
* FRSIRT: ADV-2008-0514
http://www.frsirt.com/english/advisories/2008/0514/references
* SECTRACK: 1019376
http://www.securitytracker.com/id?1019376
* SECUNIA: 28906
http://secunia.com/advisories/28906

CVE Reference: CVE-2008-0102

❖ 16855 Mini-Redirector Heap Overflow Vulnerability (MS08-007/946026) (Remote File Checking)

A remote code execution vulnerability exists in the way that the WebDAV Mini-Redirector handles responses. 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.

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

References:

* MS: MS08-007
http://www.microsoft.com/technet/security/bulletin/ms08-007.mspx
* CERT: TA08-043C
http://www.us-cert.gov/cas/techalerts/TA08-043C.html
* BID: 27670
http://www.securityfocus.com/bid/27670
* FRSIRT: ADV-2008-0509
http://www.frsirt.com/english/advisories/2008/0509/references
* SECTRACK: 1019372
http://www.securitytracker.com/id?1019372
* SECUNIA: 28894
http://secunia.com/advisories/28894

CVE Reference: CVE-2008-0080

❖ 16854 OLE Heap Overrun Vulnerability (MS08-008/947890) (Remote File Checking)

A remote code execution vulnerability exists in Object Linking and Embedding (OLE) Automation that could allow an attacker who successfully exploited this vulnerability to make changes to the system with the permissions of the logged-on user. If a user is logged on with administrative user rights, an attacker could take complete control of the 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 impacted than users who operate with administrative user rights.

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

References:

* MS: MS08-008
http://www.microsoft.com/technet/security/bulletin/ms08-008.mspx
* CERT: TA08-043C
http://www.us-cert.gov/cas/techalerts/TA08-043C.html
* BID: 27661
http://www.securityfocus.com/bid/27661
* FRSIRT: ADV-2008-0510
http://www.frsirt.com/english/advisories/2008/0510/references
* SECTRACK: 1019373
http://www.securitytracker.com/id?1019373
* SECUNIA: 28902
http://secunia.com/advisories/28902

CVE Reference: CVE-2007-0065

❖ 16853 ActiveX Object Memory Corruption Vulnerability (MS08-010/944533) (Remote File Checking)

A remote code execution vulnerability exists in a component of Microsoft Fox Pro. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

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

References:

* MILW0RM: 4369
http://www.milw0rm.com/exploits/4369
* MS: MS08-010
http://www.microsoft.com/technet/security/bulletin/ms08-010.mspx
* CERT: TA08-043C
http://www.us-cert.gov/cas/techalerts/TA08-043C.html
* BID: 25571
http://www.securityfocus.com/bid/25571
* FRSIRT: ADV-2008-0512
http://www.frsirt.com/english/advisories/2008/0512/references
* SECTRACK: 1019378
http://www.securitytracker.com/id?1019378
* XF: foxpro-fpole-activex-bo(36496)
http://xforce.iss.net/xforce/xfdb/36496

CVE Reference: CVE-2007-4790

❖ 16852 Argument Handling Memory Corruption Vulnerability (MS08-010/944533) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer handles argument validation in image processing. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

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

References:

* MS: MS08-010
http://www.microsoft.com/technet/security/bulletin/ms08-010.mspx
* CERT: TA08-043C
http://www.us-cert.gov/cas/techalerts/TA08-043C.html
* BID: 27689
http://www.securityfocus.com/bid/27689
* FRSIRT: ADV-2008-0512
http://www.frsirt.com/english/advisories/2008/0512/references
* SECTRACK: 1019381

http://www.securitytracker.com/id?1019381
* SECUNIA: 28903
http://secunia.com/advisories/28903

CVE Reference: CVE-2008-0078

❖ 16851 Property Memory Corruption Vulnerability (MS08-010/944533) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer handles a property method. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

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

References:

* MS: MS08-010
http://www.microsoft.com/technet/security/bulletin/ms08-010.mspx
* CERT: TA08-043C
http://www.us-cert.gov/cas/techalerts/TA08-043C.html
* BID: 27666
http://www.securityfocus.com/bid/27666
* FRSIRT: ADV-2008-0512
http://www.frsirt.com/english/advisories/2008/0512/references
* SECTRACK: 1019380
http://www.securitytracker.com/id?1019380
* SECUNIA: 28903
http://secunia.com/advisories/28903

CVE Reference: CVE-2008-0077

❖ 16850 HTML Rendering Memory Corruption Vulnerability (MS08-010/944533) (Remote File Checking)

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. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

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

References:

* MS: MS08-010
http://www.microsoft.com/technet/security/bulletin/ms08-010.mspx
* CERT: TA08-043C
http://www.us-cert.gov/cas/techalerts/TA08-043C.html

* BID: 27668
http://www.securityfocus.com/bid/27668
* FRSIRT: ADV-2008-0512
http://www.frsirt.com/english/advisories/2008/0512/references
* SECTRACK: 1019379
http://www.securitytracker.com/id?1019379
* SECUNIA: 28903
http://secunia.com/advisories/28903

CVE Reference: CVE-2008-0076

New Vulnerabilities found this Week

Cisco Unified IP Phone Multiple Vulnerabilities

"Denial of Service"

Some vulnerabilities have been reported in Cisco Unified IP Phone models, which can be exploited by malicious users to compromise a vulnerable device or by malicious people to cause a DoS (Denial of Service) and compromise a vulnerable device.

1) A boundary error within the internal SSH server can be exploited to cause a buffer overflow via a specially crafted packet sent to default port 22/TCP.

2) A boundary error in the parsing of DNS responses can be exploited to cause a buffer overflow.

3) A boundary error in the handling of MIME encoded data can be exploited to cause a buffer overflow via a specially crafted SIP message.

Successful exploitation of the vulnerabilities may allow execution of arbitrary code.

4) A boundary error within the internal telnet server can be exploited to cause a buffer overflow via a specially crafted command.

Successful exploitation may allow execution of arbitrary code but requires that the telnet server is enabled (not enabled by default).

5) A boundary error in the handling of challenge/response messages from an SIP proxy can be exploited to cause a heap-based buffer overflow.

Successful exploitation may allow execution of arbitrary code but requires e.g. control of a SIP proxy.

6) An error in the handling of ICMP echo request packets can be exploited to cause a device to reboot via an overly large ICMP echo request packet.

7) An error within the internal HTTP server when handling HTTP requests can be exploited to cause the device to reboot via a specially crafted HTTP request.

References:
http://www.cisco.com/warp/public/707/cisco-sa-20080213-phone.shtml

PCRE Character Class Buffer Overflow

"Denial of Service"

A vulnerability has been reported in PCRE, which potentially can be exploited by malicious people to cause a DoS (Denial of Service) or compromise an application using the library.

The vulnerability is caused due to a boundary error when processing character classes and can be exploited to cause a buffer overflow via an overly long character class with codepoints greater than 255.

The vulnerability is reported in versions prior to 7.6.

References:
http://pcre.org/changelog.txt

Linux Kernel "vmsplice()" System Call Vulnerabilities

"Denial of Service; Disclose potentially sensitive information; Gain escalated privileges"

Some vulnerabilities have been reported in the Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service), disclose potentially sensitive information, and gain escalated privileges.

The vulnerabilities are caused due to the missing verification of parameters within the "vmsplice_to_user()", "copy_from_user_mmap_sem()", and "get_iovec_page_array()" functions in fs/splice.c before using them to perform certain memory operations. This can be exploited to e.g. read or write to arbitrary kernel memory via a specially crafted "vmsplice()" system call.

Successful exploitation allows attackers to e.g. gain "root" privileges.

Note: The affected system call first appeared in version 2.6.17.

References:
http://www.isec.pl/vulnerabilities/isec-0026-vmsplice_to_kernel.txt

Adobe Flash Media Server Edge Server Multiple Vulnerabilities

"Execution of arbitrary code"

Some vulnerabilities have been reported in Adobe Flash Media Server, which can be exploited by malicious people to compromise a vulnerable system.

1) Integer overflow errors in the Edge Server component when parsing RTMP (Real Time Message Protocol) messages can be exploited to cause a heap-based buffer overflow via specially crafted packets sent to default ports 1935/TCP or 19350/TCP.

2) An error in the Edge Server component when parsing RTMP messages can be exploited to cause a memory corruption by sending a certain sequence of requests.

Successful exploitation of the vulnerabilities allows execution of arbitrary code.

The vulnerabilities affect versions 2.0.4 and prior.

References:
http://www.adobe.com/support/security/bulletins/apsb08-03.html

Microsoft patch Tuesday

This week Microsoft released updates to solve the following issues:

Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code Execution (946026)
Vulnerability in OLE Automation Could Allow Remote Code Execution (947890)
Vulnerability in Microsoft Word Could Allow Remote Code Execution (947077)
Cumulative Security Update for Internet Explorer (944533)
Vulnerabilities in Microsoft Office Publisher Could Allow Remote Code Execution (947085)
Vulnerability in Microsoft Office Could Allow Remote Code Execution (947108)
Vulnerability in Active Directory Could Allow Denial of Service (946538)
Vulnerability in Windows TCP/IP Could Allow Denial of Service (946456)
Vulnerability in Internet Information Services Could Allow Elevation of Privilege (942831)
Vulnerability in Internet Information Services Could Allow Remote Code Execution (942830)
Vulnerabilities in Microsoft Works File Converter Could Allow Remote Code Execution (947081)

References:
http://www.microsoft.com/technet/security/bulletin/ms08-feb.mspx
http://descriptions.securescout.com/tc/16850
http://descriptions.securescout.com/tc/16851
http://descriptions.securescout.com/tc/16852
http://descriptions.securescout.com/tc/16853
http://descriptions.securescout.com/tc/16854
http://descriptions.securescout.com/tc/16855
http://descriptions.securescout.com/tc/16856
http://descriptions.securescout.com/tc/16857
http://descriptions.securescout.com/tc/16858
http://descriptions.securescout.com/tc/16859

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