netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 15

April 11, 2008

Table of Contents

Product Focus

Much anticipated "Negev" in public Beta.

Try the New Beta Perimeter system, our Web-interface for the Perimeter Service is now running dynamic pages based on "Ajax", giving a much improved response time and customer experience. Existing customers can log right into the new system from the usual login page, The rest of you should contact sales for a free trial.

Mydoom Worm Scanner – The S4 MyDoom Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any have been infected by the MyDoom email virus or its variants.

CTO Jesper Jurcenoks of netVigilance is the keynote speaker at the ITEC Conference & Exhibition 2008 in Houston May 8, see
http://www.netvigilance.com/events

This Week in Review

New report shows the web is the primary target for attacks. More than 1/2 of UK websites vulnerable. Encryption just not that perfect. Some of the most distinguished cryptographers meet.

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

- **Malicious Attacks Focused Toward Trusted Web Sites**

Symantec Report Reveals Malicious Attacks Focused Toward Trusted Web Sites
New Internet Security Threat Report Reveals Details on Hackers' Quest for Private Information

The latest Internet Security Threat Report (ISTR), Volume XIII released today by Symantec Corp. (Nasdaq: SYMC) concludes that the web is now the primary conduit of attack activity, as opposed to network attacks, and that online users can increasingly be infected simply by visiting everyday web sites. The report is derived from data collected by millions of internet sensors, first-hand research and active monitoring of hacker communications and provides a global view of the state of internet security.

scoop

Full Story :
http://www.scoop.co.nz/stories/SC0804/S00022.htm

- **60% of UK websites plagued by encryption and cross-site scripting vulnerabilities**

Web application security tests show that 60% of UK sites are plagued with internet encryption and cross-site scripting vulnerabilities.
The finding forms part of NTA's Annual Web Application Security Report 2008, which analysed data gathered from web application security tests performed for a wide range of industry sectors, including finance, government, education, IT, law and retail.

In addition, the security tests found that more than three-quarters (78%) of websites tested contained one or more medium-level risk that may enable external users to gain unauthorised access or disrupt service availability.

computerweekly

Full Story :
http://www.computerweekly.com/Articles/2008/04/09/230213/60-of-uk-websites-plagued-by-encryption-and-cross-site-scripting.htm

- **Memory trick breaks PC encryption**

Encrypted information held on a laptop is more vulnerable than previously thought, US research has shown.
Scientists have shown that it is possible to recover the key that unscrambles data from a PC's memory.

It was previously thought that data held in so-called "volatile memory" was only retained

for a few seconds after the machine was switched off.

But the team found that data including encryption keys could be held and retrieved for up to several minutes.

Bbc news

Full Story :
http://news.bbc.co.uk/1/hi/technology/7275407.stm

- **Cryptographers speak of threats, voting, and Blu-Ray rumors**

On Tuesday, the creators of the Diffie-Hellman key exchange, a cryptographic protocol, and two of the creators of EMC security division RSA gathered onstage for the annual cryptographers' panel at RSA 2008 in San Francisco.

First, panel members offered their perspectives on the state of security since last year, then they answered questions posed by a moderator. The panel included: Whitfield Diffie, chief security officer at Sun Microsystems; Martin Hellman, professor emeritus of electrical engineering at Stanford University; Ronald Rivest, professor of electrical engineering and computer science at MIT; and Adi Shamir, professor of computer science at the Weizmann Institute of Science in Israel. The moderator was by Burt Kaliski, founding scientist at RSA Laboratories.

Cnet news

Full Story :
http://www.news.com/8301-10789_3-9914553-57.html?part=rss&subj=news&tag=2547-1001_3-0-5

New Vulnerabilities Tested in SecureScout

- **16086 Trillian Heap-based buffer overflow in the XMPP component (Remote File Checking)**

Heap-based buffer overflow in the Rendezvous / Extensible Messaging and Presence Protocol (XMPP) component (plugins\rendezvous.dll) for Cerulean Studios Trillian Pro before 3.1.5.1 allows remote attackers to execute arbitrary code via a message that triggers the overflow from expansion that occurs during encoding.

The vulnerability is reported fixed in version 3.1.5.1.

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

Some References:

* BUGTRAQ: 20070502 TPTI-07-06: Trillian Pro Rendezvous XMPP HTML Decoding Heap Corruption
http://www.securityfocus.com/archive/1/archive/1/467439/100/0/threaded
* MISC:
http://dvlabs.tippingpoint.com/advisory/TPTI-07-06

* CONFIRM:
http://blog.ceruleanstudios.com/?p=131
* BID: 23781
http://www.securityfocus.com/bid/23781
* XF: trillian-xmpp-bo(34059)
http://xforce.iss.net/xforce/xfdb/34059

CVE Reference: CVE-2007-2418

❖ **16903 Project Memory Validation Vulnerability (MS08-018/950183) (Remote File Checking)**

A remote code execution vulnerability exists in the way Microsoft Project handles specially crafted Project files. An attacker could exploit the vulnerability by sending a malformed file which could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

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:

* MS: MS08-018
http://www.microsoft.com/technet/security/bulletin/ms08-018.mspx
* CERT-VN: VU#155563
http://www.kb.cert.org/vuls/id/155563
* BID: 28607
http://www.securityfocus.com/bid/28607
* FRSIRT: ADV-2008-1142
http://www.frsirt.com/english/advisories/2008/1142/references
* SECTRACK: 1019797
http://www.securitytracker.com/id?1019797
* SECUNIA: 29690
http://secunia.com/advisories/29690
* XF: project-file-code-execution(41447)
http://xforce.iss.net/xforce/xfdb/41447

CVE Reference: CVE-2008-1088

❖ **16904 GDI Heap Overflow Vulnerability (MS08-021/948590) (Remote File Checking)**

A remote code execution vulnerability exists in the way that GDI handles integer calculations. The vulnerability could allow remote code execution if a user opens a specially crafted EMF or WMF image file. 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: MS08-021
http://www.microsoft.com/technet/security/bulletin/ms08-021.mspx
* BID: 28571
http://www.securityfocus.com/bid/28571
* FRSIRT: ADV-2008-1145
http://www.frsirt.com/english/advisories/2008/1145/references
* SECTRACK: 1019798
http://www.securitytracker.com/id?1019798
* SECUNIA: 29704
http://secunia.com/advisories/29704
* XF: win-emf-wmf-header-bo(41471)
http://xforce.iss.net/xforce/xfdb/41471

CVE Reference: CVE-2008-1083

❖ 16905 GDI Stack Overflow Vulnerability (MS08-021/948590) (Remote File Checking)

A remote code execution vulnerability exists in the way that GDI handles filename parameters in EMF files. The vulnerability could allow remote code execution if a user opens a specially crafted EMF image file. 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: MS08-021
http://www.microsoft.com/technet/security/bulletin/ms08-021.mspx
* BID: 28570
http://www.securityfocus.com/bid/28570
* FRSIRT: ADV-2008-1145
http://www.frsirt.com/english/advisories/2008/1145/references
* SECTRACK: 1019798
http://www.securitytracker.com/id?1019798
* SECUNIA: 29704
http://secunia.com/advisories/29704

CVE Reference: CVE-2008-1087

❖ 16906 VBScript/JScript Remote Code Execution Vulnerability (MS08-022/944338) (Remote File Checking)

A remote code execution vulnerability exists in the way that the VBScript and JScript scripting engines decode script in Web pages. This vulnerability could allow remote code execution if a user opened a specially crafted file or visited a Web site that is running specially crafted script. If a user is 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 impacted than users who operate with administrative user rights.

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

References:

* MS: MS08-022
http://www.microsoft.com/technet/security/bulletin/ms08-022.mspx
* BID: 28551
http://www.securityfocus.com/bid/28551
* FRSIRT: ADV-2008-1146
http://www.frsirt.com/english/advisories/2008/1146/references
* SECTRACK: 1019799
http://www.securitytracker.com/id?1019799
* SECUNIA: 29712
http://secunia.com/advisories/29712

CVE Reference: CVE-2008-0083

❖ 16908 Data Stream Handling Memory Corruption Vulnerability (MS08-024/947864) (Remote File Checking)

A remote code execution vulnerability exists in Internet Explorer because of the way that it processes data streams. 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:

* MISC:
http://secunia.com/secunia_research/2007-100/advisory/
* MS: MS08-024
http://www.microsoft.com/technet/security/bulletin/ms08-024.mspx
* BID: 28552
http://www.securityfocus.com/bid/28552
* FRSIRT: ADV-2008-1148

http://www.frsirt.com/english/advisories/2008/1148/references
* SECTRACK: 1019801
http://www.securitytracker.com/id?1019801
* SECUNIA: 27707
http://secunia.com/advisories/27707

CVE Reference: CVE-2008-1085

❖ 16909 DNS Spoofing Attack Vulnerability (MS08-020/945553) (Remote File Checking)

A spoofing vulnerability exists in Windows DNS clients. The vulnerability could allow an unauthenticated attacker to send malicious responses to DNS requests made by vulnerable clients, thereby spoofing or redirecting Internet traffic from legitimate locations.

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

References:

* MS: MS08-020
http://www.microsoft.com/technet/security/bulletin/ms08-020.mspx
* BID: 28553
http://www.securityfocus.com/bid/28553
* FRSIRT: ADV-2008-1144
http://www.frsirt.com/english/advisories/2008/1144/references
* SECTRACK: 1019802
http://www.securitytracker.com/id?1019802
* SECUNIA: 29696
http://secunia.com/advisories/29696

CVE Reference: CVE-2008-0087

❖ 16910 Windows Kernel Vulnerability (MS08-025/941693) (Remote File Checking)

An elevation of privilege vulnerability exists due to the Windows kernel improperly validating input passed from user mode to the kernel. The vulnerability could allow an attacker to run code with elevated privileges. An attacker who successfully exploited this vulnerability could execute arbitrary code and 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: MS08-025
http://www.microsoft.com/technet/security/bulletin/ms08-025.mspx
* BID: 28554
http://www.securityfocus.com/bid/28554
* FRSIRT: ADV-2008-1149

http://www.frsirt.com/english/advisories/2008/1149/references
* SECTRACK: 1019803
http://www.securitytracker.com/id?1019803
* SECUNIA: 29720
http://secunia.com/advisories/29720

CVE Reference: CVE-2008-1084

❖ 16911 Visio Object Header Vulnerability (MS08-019/949032) (Remote File Checking)

A remote code execution vulnerability exists in the way Microsoft Visio validates object header data in specially crafted files. An attacker could exploit the vulnerability by sending a malformed file which could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

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:

* MS: MS08-019
http://www.microsoft.com/technet/security/Bulletin/MS08-019.mspx
* BID: 28555
http://www.securityfocus.com/bid/28555
* FRSIRT: ADV-2008-1143
http://www.frsirt.com/english/advisories/2008/1143/references
* SECTRACK: 1019804
http://www.securitytracker.com/id?1019804
* SECUNIA: 29691
http://secunia.com/advisories/29691
* XF: visio-object-header-code-execution(41451)
http://xforce.iss.net/xforce/xfdb/41451

CVE Reference: CVE-2008-1089

❖ 16912 Visio Memory Validation Vulnerability (MS08-019/949032) (Remote File Checking)

A remote code execution vulnerability exists in the way Microsoft Visio validates memory allocations when loading specially-crafted .DXF files from disk into memory. An attacker could exploit the vulnerability by sending a malformed file which could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

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:

* MS: MS08-019
http://www.microsoft.com/technet/security/Bulletin/MS08-019.mspx
* BID: 28555
http://www.securityfocus.com/bid/28555
* FRSIRT: ADV-2008-1143
http://www.frsirt.com/english/advisories/2008/1143/references
* SECTRACK: 1019804
http://www.securitytracker.com/id?1019804
* SECUNIA: 29691
http://secunia.com/advisories/29691
* XF: visio-object-header-code-execution(41451)
http://xforce.iss.net/xforce/xfdb/41451

CVE Reference: CVE-2008-1089

New Vulnerabilities found this Week

Microsoft Patch Tuesday

This Tuesday, Microsoft released patches for the following vulnerabilities:

Project Memory Validation Vulnerability (MS08-018/950183)
GDI Heap Overflow Vulnerability (MS08-021/948590)
GDI Stack Overflow Vulnerability (MS08-021/948590)
VBScript/JScript Remote Code Execution Vulnerability (MS08-022/944338)
ActiveX Object Memory Corruption Vulnerability (MS08-023/948881)
Data Stream Handling Memory Corruption Vulnerability (MS08-024/947864)
DNS Spoofing Attack Vulnerability (MS08-020/945553)
Windows Kernel Vulnerability (MS08-025/941693)
Visio Object Header Vulnerability (MS08-019/949032)
Visio Memory Validation Vulnerability (MS08-019/949032)

References:
http://www.microsoft.com/technet/security/Bulletin/MS08-018.mspx
http://www.microsoft.com/technet/security/bulletin/ms08-021.mspx
http://www.microsoft.com/technet/security/Bulletin/ms08-022.mspx
http://www.microsoft.com/technet/security/bulletin/ms08-023.mspx
http://www.microsoft.com/technet/security/bulletin/ms08-024.mspx
http://www.microsoft.com/technet/security/bulletin/ms08-020.mspx
http://www.microsoft.com/technet/security/bulletin/ms08-025.mspx

http://www.microsoft.com/technet/security/Bulletin/MS08-019.mspx

Lotus Notes Multiple Keyview Parsing Vulnerabilities
"Buffer overflows"

Secunia Research has discovered some vulnerabilities in Lotus Notes, which can be exploited by malicious people to compromise a user's system.

The vulnerabilities are caused due to various errors within certain third-party file viewers and can be exploited to cause buffer overflows when a specially crafted file attachment is viewed.

The vulnerabilities are confirmed in versions 7.0.3 and 8.0. Other versions may also be affected.

References:
http://www.ibm.com/support/docview.wss?rs=463&uid=swg21298453

Adobe Flash Player Multiple Vulnerabilities
"Heap-based buffer overflow; Integer overflow; Execution of arbitrary code"

Some vulnerabilities have been reported in Adobe Flash Player, which can be exploited by malicious people to bypass certain security restrictions, conduct cross-site scripting attacks, or to potentially compromise a user's system.

1) A boundary error exists in the processing of "Declare Function (V7)" tags. This can be exploited to cause a heap-based buffer overflow via specially crafted flags.

2) An integer overflow in the processing of multimedia files can be exploited to cause a buffer overflow.

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

3) Errors when pinning a hostname to an IP address can be exploited to conduct DNS rebinding attacks.

4) An error when sending HTTP headers can be exploited to bypass cross-domain policy files.

5) An error exists in the enforcing of cross-domain policy files. This can be exploited to bypass certain security restrictions on web servers hosting cross-domain policy files.

6) Input passed to unspecified parameters when handling e.g. the "asfunction:" protocol is not properly sanitised before being returned to the user. This can be exploited to inject arbitrary HTML and script code in a user's browser session in context of an affected site.

The vulnerabilities are reported in versions prior to 9.0.124.0.

References:
http://www.adobe.com/support/security/bulletins/apsb08-11.html

HP OpenView Network Node Manager ovspmd.exe Buffer Overflow
"Denial of Service; Execution of arbitrary code"

Luigi Auriemma has discovered a vulnerability in HP OpenView Network Node Manager, which can be exploited by malicious people to cause a DoS (Denial of Service) or potentially compromise a vulnerable system.

The vulnerability is caused due to an input validation error within ovspmd.exe and can be exploited to cause a heap-based buffer overflow by sending a specially crafted, overly long packet to default port 8886/TCP.

Successful exploitation may allow execution of arbitrary code.

The vulnerability is confirmed in version 7.53 and 7.51. Other versions may also be affected.

References:
http://aluigi.altervista.org/adv/closedview-adv.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