

Table of Contents

[Product Focus](#)

[This Week in Review](#)

[Top Security News Stories this Week](#)

[New Vulnerabilities Tested in SecureScout](#)

[New Vulnerabilities found this Week](#)

Product Focus

[Task Scheduler Vulnerability Scanner](#) - The S4 Task Scheduler Vulnerability 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 Task Scheduler flaw (MS04-022).

Download Here:

<http://www.netvigilance.com/productdownloads?productname=taskschedulervulnerabilityscanner>

This Week in Review

Need for US cyberattack plan. Power grid protection. New 911 service launched. Where does US cybersecurity belong?

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

• National Academy of Sciences says U.S. needs cyberattack plan

U.S. cyber capabilities are at least as powerful as its most sophisticated adversary, but the country needs a clear plan should it decide to unleash a digital attack of its own, according to a report from the National Academy of Sciences (NAS) released Wednesday.

The report, entitled "Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities," said a number of challenges lie ahead, including developing rules for the use of cyberweapons, coordinating allied nations and public and private entities, determining the outcome of cyberattacks on enemies and dealing with the possible "significant" operational implications a cyberattack could have on the U.S. private sector.

The report concluded that a national debate about cyberattack policy should be fostered, and the U.S. government should organize the decision-making process for engaging in a cyberattack.

Full Story :

<http://www.scmagazineus.com/National-Academy-of-Sciences-says-US-needs-cyberattack-plan/article/131653/>

• **Planned legislation to protect power grid**

Updated Wednesday, April 29, 2009 at 4:56 p.m. EST

Not long after reports surfaced that foreign spies have penetrated the U.S. power grid, lawmakers are planning to introduce a bill Thursday aimed at creating standards to protect the nation's critical electric infrastructure.

The Critical Electric Infrastructure Protection Act is scheduled to be introduced by Sen. Joseph Lieberman, I-Conn., chairman of the U.S. Senate Committee on Homeland Security and Governmental Affairs, and Rep. Bennie Thompson, D-Miss., chairman of the U.S. House Committee on Homeland Security.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Planned-legislation-to-protect-power-grid/article/131596/>

• **"Online 911" created to diagnose and deal with cybercrime**

When someone becomes the victim of cybercrime, it's often hard to know what to do next or to whom to turn. Even worse, people often don't even know they're a victim.

In response to these issues, McAfee on Tuesday launched a free Cybercriminal Response Unit (CRU), meant to serve as "online 911" where cybercrime is diagnosed and dealt with, Pamela Warren, McAfee's chief cybercrime strategist, told SCMagazineUS.com Monday.

The CRU is aimed at helping consumers and small businesses -- whether users believe they have clicked on a malicious link or have a child that is being cyber-bullied, the CRU can tell users where to turn for help. The site also provides resources to deal with a number of other problem scenarios, including stolen laptops, cyberstalking, online predators, and pop-up ads.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Online-911-created-to-diagnose-and-deal-with-cybercrime/article/131476/>

• **Policymakers debate White House's role in cybersecurity**

Lawmakers and public policy experts clashed Tuesday at a U.S. Senate committee hearing over whether cybersecurity control should be taken away from the U.S. Department of Homeland Security (DHS) and placed under the White House's purview.

The Committee on Homeland Security and Governmental Affairs heard testimony about whether an executive White House office in charge of cybersecurity coordination should be created, as recommended by the Commission on Cybersecurity for the 44th Presidency in December. That report said that a new National Office for Cyberspace (NOC), an executive White House office in charge of cybersecurity coordination, was essential for the United States.

Many have praised the commission's recommendations, but Stewart Baker, former assistant secretary of the DHS said Tuesday that he questions how effective and efficient a reorganization of government cybersecurity coordination would be.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Policymakers-debate-White-Houses-role-in-cybersecurity/article/131513/>

New Vulnerabilities Tested in SecureScout

• **18352 Windows HTTP Services Credential Reflection Vulnerability (MS09-013/960803) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Windows HTTP Services handles NTLM credentials when a user connects to an attacker's Web server. This vulnerability allows an attacker to replay the user's credentials back to the attacker and execute code in the context of the logged-on user. 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: MS09-013
<http://www.microsoft.com/technet/security/Bulletin/MS09-013.msp>
- * MS: MS09-014
<http://www.microsoft.com/technet/security/Bulletin/MS09-014.msp>
- * CERT: TA09-104A
<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>
- * OSVDB: 53619
<http://osvdb.org/53619>
- * SECTRACK: 1022041
<http://www.securitytracker.com/id?1022041>
- * SECUNIA: 34677
<http://secunia.com/advisories/34677>
- * SECUNIA: 34678
<http://secunia.com/advisories/34678>
- * VUPEN: ADV-2009-1027
<http://www.vupen.com/english/advisories/2009/1027>
- * VUPEN: ADV-2009-1028
<http://www.vupen.com/english/advisories/2009/1028>

CVE Reference:

CVE-2009-0550 (cve.mitre.org, nvd.nist.gov)

• **18353 WordPad and Office Text Converter Memory Corruption Vulnerability (MS09-010/960477) (Remote File Checking)**

A remote code execution vulnerability exists in the way that text converters in WordPad and Microsoft Office process memory when a user opens a specially crafted Word 6 file that includes malformed data.

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

References:

- * MS: MS09-010
<http://www.microsoft.com/technet/security/Bulletin/MS09-010.msp>
- * CERT: TA09-104A
<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>
- * OSVDB: 53662
<http://osvdb.org/53662>
- * SECTRACK: 1022043
<http://www.securitytracker.com/id?1022043>
- * VUPEN: ADV-2009-1024
<http://www.vupen.com/english/advisories/2009/1024>

CVE Reference:

CVE-2009-0087 (cve.mitre.org, nvd.nist.gov)

• **18354 WordPad Word 97 Text Converter Stack Overflow Vulnerability (CVE-2008-4841) (MS09-010/960477) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft WordPad processes memory when parsing a specially crafted Word 97 document. The vulnerability could allow remote code execution if a user opens a specially crafted Word file that includes a malformed list structure.

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

References:

- * MILWORM: 6560
<http://www.milw0rm.com/exploits/6560>
- * MISC:
<http://milw0rm.com/spl0its/2008-crash.doc.rar>
- * CONFIRM:
<http://www.microsoft.com/technet/security/advisory/960906.msp>
- * MS: MS09-010
<http://www.microsoft.com/technet/security/Bulletin/MS09-010.msp>
- * CERT: TA09-104A
<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>

* BID: 31399
<http://www.securityfocus.com/bid/31399>
* BID: 32718
<http://www.securityfocus.com/bid/32718>
* VUPEN: ADV-2008-3390
<http://www.frsirt.com/english/advisories/2008/3390>
* SECTRACK: 1021376
<http://securitytracker.com/id?1021376>
* SECUNIA: 32997
<http://secunia.com/advisories/32997>
* SREASON: 4711
<http://securityreason.com/securityalert/4711>
* VUPEN: ADV-2009-1024
<http://www.vupen.com/english/advisories/2009/1024>

CVE Reference:

CVE-2008-4841 (cve.mitre.org, nvd.nist.gov)
CVE-2008-4841 (cve.mitre.org, nvd.nist.gov)

• **18355 Word 2000 WordPerfect 6.x Converter Stack Corruption Vulnerability (MS09-010/960477) (Remote File Checking)**

A remote code execution vulnerability exists in the way that the WordPerfect 6.x converter that is included with Microsoft Office Word 2000 processes memory when parsing a specially crafted WordPerfect document.

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

References:

* MS: MS09-010
<http://www.microsoft.com/technet/security/Bulletin/MS09-010.msp>
* CERT: TA09-104A
<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>
* OSVDB: 53663
<http://osvdb.org/53663>
* SECTRACK: 1022043
<http://www.securitytracker.com/id?1022043>
* VUPEN: ADV-2009-1024
<http://www.vupen.com/english/advisories/2009/1024>

CVE Reference:

CVE-2009-0088 (cve.mitre.org, nvd.nist.gov)

• **18356 WordPad Word 97 Text Converter Stack Overflow Vulnerability (CVE-2009-0235) (MS09-010/960477) (Remote File Checking)**

A remote code execution vulnerability exists in WordPad as a result of memory corruption when a user opens a specially crafted Word file.

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

References:

* IDEFENSE: 20090414 Microsoft WordPad Word97 Converter Stack Buffer Overflow Vulnerability
<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=783>
* MS: MS09-010
<http://www.microsoft.com/technet/security/Bulletin/MS09-010.msp>
* CERT: TA09-104A
<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>
* BID: 34470
<http://www.securityfocus.com/bid/34470>
* OSVDB: 53664
<http://osvdb.org/53664>
* SECTRACK: 1022043
<http://www.securitytracker.com/id?1022043>
* VUPEN: ADV-2009-1024
<http://www.vupen.com/english/advisories/2009/1024>

CVE Reference:

CVE-2009-0235 (cve.mitre.org, nvd.nist.gov)

• 18357 Microsoft DirectShow MJPEG Decompression Vulnerability (MS09-011/961373) (Remote File Checking)

A remote code execution vulnerability exists in the way Microsoft DirectShow handles supported format files. This vulnerability could allow code execution if a user opened a specially crafted MJPEG file. 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:

- * MISC:
<http://www.piotrbania.com/all/adv/ms-directx-mjpeg-adv.txt>
- * CONFIRM:
<http://support.avaya.com/elmodocs2/security/ASA-2009-132.htm>
- * MS: MS09-011
<http://www.microsoft.com/technet/security/Bulletin/MS09-011.mspx>
- * CERT: TA09-104A
<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>
- * BID: 34460
<http://www.securityfocus.com/bid/34460>
- * OSVDB: 53632
<http://osvdb.org/53632>
- * SECTRACK: 1022040
<http://www.securitytracker.com/id?1022040>
- * SECUNIA: 34665
<http://secunia.com/advisories/34665>
- * VUPEN: ADV-2009-1025
<http://www.vupen.com/english/advisories/2009/1025>

CVE Reference:

CVE-2009-0084 (cve.mitre.org, nvd.nist.gov)

• 18358 Windows MSDTC Service Isolation Vulnerability (MS09-012/959454) (Remote File Checking)

An elevation of privilege vulnerability exists in the Microsoft Distributed Transaction Coordinator (MSDTC) transaction facility in Microsoft Windows platforms. MSDTC leaves a NetworkService token that can be impersonated by any process that calls into it. The vulnerability allows a process that is not running under the NetworkService account, but that has the SeImpersonatePrivilege, to elevate its privilege to NetworkService and execute code with NetworkService 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:

- * BUGTRAQ: 20081008 Token Kidnapping Windows 2003 PoC exploit
<http://www.securityfocus.com/archive/1/archive/1/497168/100/0/threaded>
- * BUGTRAQ: 20080419 Token Kidnapping (Microsoft Security Advisory 951306) presentation available
<http://www.securityfocus.com/archive/1/archive/1/491111/100/0/threaded>
- * MILWORM: 6705
<http://www.milw0rm.com/exploits/6705>
- * MISC:
<http://isc.sans.org/diary.html?storyid=4306>
- * MISC:
<http://milw0rm.com/spl0its/2008-Churrasco.zip>
- * MISC:
<http://nomoreroot.blogspot.com/2008/10/windows-2003-poc-exploit-for-token.html>
- * MISC:
http://securitywatch.eweek.com/flaws/microsoft_belatedly_admits_to_windows_server_2008_token_kidnapping.html
- * MISC:
<http://www.argeniss.com/research/Churrasco.zip>
- * MISC:
<http://www.argeniss.com/research/TokenKidnapping.pdf>
- * CONFIRM:
<http://blogs.technet.com/msrc/archive/2008/04/17/msrc-blog-microsoft-security-advisory-951306.aspx>
- * CONFIRM:

<http://www.microsoft.com/technet/security/advisory/951306.msp>

* MS: MS09-012

<http://www.microsoft.com/technet/security/bulletin/ms09-012.msp>

* CERT: TA09-104A

<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>

* BID: 28833

<http://www.securityfocus.com/bid/28833>

* VUPEN: ADV-2008-1264

<http://www.frsirt.com/english/advisories/2008/1264/references>

* SECTRACK: 1019904

<http://www.securitytracker.com/id?1019904>

* SECUNIA: 29867

<http://secunia.com/advisories/29867>

* VUPEN: ADV-2009-1026

<http://www.vupen.com/english/advisories/2009/1026>

* XF: ms-windows-localsystem-privilege-escalation(41880)

<http://xforce.iss.net/xforce/xfdb/41880>

CVE Reference:

CVE-2008-1436 (cve.mitre.org, nvd.nist.gov)

• 18359 Windows WMI Service Isolation Vulnerability (MS09-012/959454) (Remote File Checking)

An elevation of privilege vulnerability exists due to the Windows Management Instrumentation (WMI) provider improperly isolating processes that run under the NetworkService or LocalService accounts. 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: MS09-012

<http://www.microsoft.com/technet/security/bulletin/ms09-012.msp>

* CERT: TA09-104A

<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>

* OSVDB: 53666

<http://osvdb.org/53666>

* VUPEN: ADV-2009-1026

<http://www.vupen.com/english/advisories/2009/1026>

CVE Reference:

CVE-2009-0078 (cve.mitre.org, nvd.nist.gov)

• 18360 Windows RPCSS Service Isolation Vulnerability (MS09-012/959454) (Remote File Checking)

An elevation of privilege vulnerability exists due to the RPCSS service improperly isolating processes that run under the NetworkService or LocalService accounts. 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: **Medium**

References:

* MS: MS09-012

<http://www.microsoft.com/technet/security/bulletin/ms09-012.msp>

* CERT: TA09-104A

<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>

* OSVDB: 53667

<http://osvdb.org/53667>

* VUPEN: ADV-2009-1026

<http://www.vupen.com/english/advisories/2009/1026>

CVE Reference:

CVE-2009-0079 (cve.mitre.org, nvd.nist.gov)

• 18361 Windows Thread Pool ACL Weakness Vulnerability (MS09-012/959454) (Remote File Checking)

An elevation of privilege vulnerability exists due to Windows placing incorrect access control lists (ACLs) on threads in the current ThreadPool. 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: **Medium**

References:

- * MS: MS09-012
<http://www.microsoft.com/technet/security/bulletin/ms09-012.msp>
- * CERT: TA09-104A
<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>
- * OSVDB: 53668
<http://osvdb.org/53668>
- * VUPEN: ADV-2009-1026
<http://www.vupen.com/english/advisories/2009/1026>

CVE Reference:

CVE-2009-0080 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-0719 HP CVSS 2.0 Score = 7.9

Unspecified vulnerability in useradd in HP HP-UX B.11.11, B.11.23, and B.11.31 allows local users to access arbitrary files and directories via unknown vectors, a different issue than CVE-2008-1660.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

- HP: <http://www.securityfocus.com/archive/1/503038>
- HP: <http://www.securityfocus.com/archive/1/503038>
- BID: <http://www.securityfocus.com/bid/34748>

CVE Reference: [CVE-2009-0719](http://cve.mitre.org/cve/2009/0719)

• CVE-2008-2438 HP CVSS 2.0 Score = 7.5

Unspecified vulnerability in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to execute arbitrary code via unknown vectors.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

- BID: <http://www.securityfocus.com/bid/34738>
- HP: <http://www.securityfocus.com/archive/1/503024>
- HP: <http://www.securityfocus.com/archive/1/503024>

CVE Reference: [CVE-2008-2438](http://cve.mitre.org/cve/2008/2438)

• CVE-2009-1430 Symantec CVSS 2.0 Score = 10.0

Multiple stack-based buffer overflows in IAO.EXE in the Intel Alert Originator Service in Symantec Alert Management System 2 (AMS2), as used in Symantec System Center (SSS); Symantec AntiVirus Server; Symantec AntiVirus Central Quarantine Server; Symantec AntiVirus (SAV) Corporate Edition 9 before 9.0 MR7, 10.0 and 10.1 before 10.1 MR8, and 10.2 before 10.2 MR2; Symantec Client Security (SCS) 2 before 2.0 MR7 and 3 before 3.1 MR8; and Symantec Endpoint Protection (SEP) before 11.0 MR3, allow remote attackers to execute arbitrary code via (1) a crafted packet or (2) data that ostensibly arrives from the MsgSys.exe process.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

- MISC: <http://www.zerodayinitiative.com/advisories/ZDI-09-018/>

CONFIRM:

http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory

BID: <http://www.securityfocus.com/bid/34674>

BID: <http://www.securityfocus.com/bid/34672>

CVE Reference: [CVE-2009-1430](#)

• **CVE-2009-1431 Symantec CVSS 2.0 Score = 10.0**

XFR.EXE in the Intel File Transfer service in the console in Symantec Alert Management System 2 (AMS2), as used in Symantec System Center (SSS); Symantec AntiVirus Server; Symantec AntiVirus Central Quarantine Server; Symantec AntiVirus (SAV) Corporate Edition 9 before 9.0 MR7, 10.0 and 10.1 before 10.1 MR8, and 10.2 before 10.2 MR2; Symantec Client Security (SCS) 2 before 2.0 MR7 and 3 before 3.1 MR8; and Symantec Endpoint Protection (SEP) before 11.0 MR3, allows remote attackers to execute arbitrary code by placing the code on a (1) share or (2) WebDAV server, and then sending the UNC share pathname to this service.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

CONFIRM:

http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory

BID: <http://www.securityfocus.com/bid/34675>

CVE Reference: [CVE-2009-1431](#)

• **CVE-2009-1429 Symantec CVSS 2.0 Score = 9.3**

The Intel LANDesk Common Base Agent (CBA) in Symantec Alert Management System 2 (AMS2), as used in Symantec System Center (SSS); Symantec AntiVirus Server; Symantec AntiVirus Central Quarantine Server; Symantec AntiVirus (SAV) Corporate Edition 9 before 9.0 MR7, 10.0 and 10.1 before 10.1 MR8, and 10.2 before 10.2 MR2; Symantec Client Security (SCS) 2 before 2.0 MR7 and 3 before 3.1 MR8; and Symantec Endpoint Protection (SEP) before 11.0 MR3, allows remote attackers to execute arbitrary commands via a crafted packet whose contents are interpreted as a command to be launched in a new process.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

CONFIRM:

http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory

BID: <http://www.securityfocus.com/bid/34671>

CVE Reference: [CVE-2009-1429](#)

• **CVE-2009-1428 Symantec CVSS 2.0 Score = 4.3**

Multiple cross-site scripting (XSS) vulnerabilities in ccLgView.exe in the Symantec Log Viewer, as used in Symantec AntiVirus (SAV) before 10.1 MR8, Symantec Endpoint Protection (SEP) 11.0 before 11.0 MR1, Norton 360 1.0, and Norton Internet Security 2005 through 2008, allow remote attackers to inject arbitrary web script or HTML via a crafted e-mail message, related to "two parsing errors."

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

CONFIRM:

http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory

BID: <http://www.securityfocus.com/bid/34669>

CVE Reference: [CVE-2009-1428](#)

• **CVE-2009-1439 Linux CVSS 2.0 Score = 7.8**

Buffer overflow in fs/cifs/connect.c in CIFS in the Linux kernel 2.6.29 and earlier allows remote attackers to cause a denial of service (crash) via a long nativeFileSystem field in a Tree Connect response to an SMB mount request.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

CONFIRM: https://bugzilla.novell.com/show_bug.cgi?id=492282

MLIST: <http://www.openwall.com/lists/oss-security/2009/04/07/7>

MLIST: <http://www.openwall.com/lists/oss-security/2009/04/07/3>

MLIST: <http://www.openwall.com/lists/oss-security/2009/04/04/1>

MLIST: <http://lists.samba.org/archive/linux-cifs-client/2009-April/004322.html>

MISC: <http://blog.fefe.de/?ts=b72905a8>

CVE Reference: [CVE-2009-1439](#)

• **CVE-2009-1190 Sun CVSS 2.0 Score = 5.0**

Algorithmic complexity vulnerability in the java.util.regex.Pattern.compile method in Sun Java Development Kit (JDK) before 1.6, when used with spring.jar in SpringSource Spring Framework 1.1.0 through 2.5.6 and 3.0.0.M1 through 3.0.0.M2 and dm Server 1.0.0 through 1.0.2, allows remote attackers to cause a denial of service (CPU consumption) via serializable data with a long regex string containing multiple optional groups, a related issue to CVE-2004-2540.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=497161

XF: <http://xforce.iss.net/xforce/xfdb/50083>

CONFIRM: <http://www.springsource.com/securityadvisory>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/502926/100/0/threaded>

MISC: http://www.packetstormsecurity.org/hitb06/DAY_1_-_Marc_Schoenefeld_-_Pentesting_Java_J2EE.pdf

SECUNIA: <http://secunia.com/advisories/34892>

CVE Reference: [CVE-2009-1190](#)

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