ScoutNews
The weekly Security update from the makers of SecureScout
December 11, 2009

2009 Issue #50

Table of Contents

Product Focus

RPC DCOM Vulnerabilities Scanner - The S4 RPC DCOM Vulnerabilities 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 Windows RPC DCOM flaws (MS03-026 and MS03-039).

Download Here:
http://www.netvigilance.com/productdownloads?productname=rpcdcomvulnerabilitiesscanner

This Week in Review

Still a long way to go with security. Cloud computing the next focus area for cyber criminals. New law for data breech victims. Help CNET pick the best electronics.

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

- **Report finds enterprises failing to protect sensitive data**

Confidential data remains unprotected in many large enterprises, according to a recent survey released by Enterprise Strategy Group (ESG) on behalf of database security firm Application Security.

In the second annual survey of 175 IT and information security professionals from North American enterprises with 1,000 or more employees, 40 percent said most of their data is adequately secured and 11 percent said some confidential data is secured. Two percent of respondents said most confidential data is not secured and another two percent said they did not know.

The remaining 40 percent of respondents said they believe that all of their organization's confidential data is adequately protected. SC Magazine

Full Story :
http://www.scmagazineus.com/report-finds-enterprises-failing-to-protect-sensitive-data/article/159260/?utm_source=

- **Trend Micro forecasts future threats**

Cloud computing and virtualization are just two technologies that cybercriminals are anxious to exploit, forecasts a report released Wednesday by security vendor Trend Micro.

The year ahead offers new opportunities for cybercrooks as they hunt for more targets and new challenges as people try to protect themselves, says Trend Micro's 2010 Future Threat Report (PDF).

Cloud computing and virtualization can be cost effective. But since they're beyond the confines of a company's own firewall, they could be potentially open areas for cybercriminals to attack. October's Sidekick data outage highlighted the vulnerabilities of the cloud, which cybercrooks are likely to abuse, according to Trend Micro. Cnet Security

Full Story :
http://news.cnet.com/8301-1009_3-10413144-83.html?part=rss&subj=news&tag=2547-1_3-0-20

- **National data breach notification bill passed in U.S. House**

A national data breach notification bill was passed in the U.S. House of Representatives on Tuesday.

The Data Accountability and Trust Act would require any organization that experiences a breach of electronic data containing personal information to notify all U.S. individuals whose information is breached. The law requires that the Federal Trade Commission to also be notified.

In addition, organizations would be required to designate an information security officer and establish a data security policy. The policy would have to address the collection of personal information and include a process for identifying and correcting system vulnerabilities and disposing electronic data. SC Magazine

Full Story :
http://www.scmagazineus.com/national-data-breach-notification-bill-passed-in-us-house/article/159404/?utm_source

- **The 20 most innovative consumer electronics products of the decade**

Recently, with the help of some of the editors here at CNET, I put together list of the biggest tech flops of the decade. Since I'm not a negative guy at heart, it was only a matter of time that I come up with a more positive spin on the whole tech-products-of-the-decade concept that's all the rage as we approach the end of '09.

Once again, I've enlisted the help of my fellow editors, so while my face may appear at the top of this list, it's really a collective effort. That said, you can blame me if you don't like the picks.

As always, feel free to suggest your own picks. If you make a good case, we'll update the list and make some changes. Also, let us know what your top 5 picks are in order of innovation and influence. Cnet Security

Full Story :
http://reviews.cnet.com/8301-18438_7-10413195-82.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

- **18620 Microsoft Internet Explorer ATL COM Initialization Vulnerability (MS09-072/976325) (Remote File Checking)**

A remote code execution vulnerability exists in an ActiveX control built with vulnerable Microsoft Active Template Library (ATL) headers. This vulnerability only directly affects systems with components and controls installed that were built using Visual Studio ATL. Components and controls built using ATL could allow the instantiation of arbitrary objects that can bypass related security policy, such as kill bits within Internet Explorer. Therefore, this vulnerability could allow a remote, unauthenticated user to perform remote code execution on an affected system. 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.

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

References:

* MISC:
http://blogs.technet.com/srd/archive/2009/08/11/ms09-037-why-we-are-using-cve-s-already-used-in-ms09-035.aspx
* CONFIRM:
http://www.adobe.com/support/security/advisories/apsa09-04.html
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb09-11.html
* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb09-13.html

* CONFIRM:
http://www.adobe.com/support/security/bulletins/apsb09-10.html
* MS: MS09-035
http://www.microsoft.com/technet/security/bulletin/ms09-035.mspx
* MS: MS09-037
http://www.microsoft.com/technet/security/Bulletin/MS09-037.mspx
* MS: MS09-055
http://www.microsoft.com/technet/security/Bulletin/MS09-055.mspx
* MS: MS09-060
http://www.microsoft.com/technet/security/Bulletin/MS09-060.mspx
* SUNALERT: 264648
http://sunsolve.sun.com/search/document.do?assetkey=1-66-264648-1
* SUNALERT: 266108
http://sunsolve.sun.com/search/document.do?assetkey=1-66-266108-1
* SUSE: SUSE-SA:2009:053
http://lists.opensuse.org/opensuse-security-announce/2009-11/msg00002.html
* CERT: TA09-195A
http://www.us-cert.gov/cas/techalerts/TA09-195A.html
* CERT: TA09-223A
http://www.us-cert.gov/cas/techalerts/TA09-223A.html
* CERT: TA09-286A
http://www.us-cert.gov/cas/techalerts/TA09-286A.html
* SECUNIA: 36187
http://secunia.com/advisories/36187
* SECUNIA: 36374
http://secunia.com/advisories/36374
* VUPEN: ADV-2009-2034
http://www.vupen.com/english/advisories/2009/2034
* VUPEN: ADV-2009-2232
http://www.vupen.com/english/advisories/2009/2232

CVE Reference:

CVE-2009-2493 (cve.mitre.org, nvd.nist.gov)

• 18621 Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability (CVE-2009-3671) (MS09-072/976325) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. 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. 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.

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

References:

* MS: MS09-072
http://www.microsoft.com/technet/security/bulletin/ms09-072.mspx
* BID: 37188
http://www.securityfocus.com/bid/37188
* VUPEN: VUPEN/ADV-2009-3437
http://www.vupen.com/english/advisories/2009/3437
* SECTRACK: 1023293
http://securitytracker.com/alerts/2009/Dec/1023293.html

CVE Reference:

CVE-2009-3671 (cve.mitre.org, nvd.nist.gov)

• 18622 Microsoft Internet Explorer HTML Object Memory Corruption Vulnerability (MS09-072/976325) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. 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. 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.

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

References:

* MS: MS09-072
http://www.microsoft.com/technet/security/bulletin/ms09-072.mspx
* BID: 37085
http://www.securityfocus.com/bid/37085
* VUPEN: VUPEN/ADV-2009-3437
http://www.vupen.com/english/advisories/2009/3437
* SECTRACK: 1023293
http://securitytracker.com/alerts/2009/Dec/1023293.html

CVE Reference:

CVE-2009-3672 (cve.mitre.org, nvd.nist.gov)

• 18623 Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability (CVE-2009-3673) (MS09-072/976325) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. 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. 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.

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

References:

* MS: MS09-072
http://www.microsoft.com/technet/security/bulletin/ms09-072.mspx
* BID: 37212
http://www.securityfocus.com/bid/37212
* VUPEN: VUPEN/ADV-2009-3437
http://www.vupen.com/english/advisories/2009/3437
* SECTRACK: 1023293
http://securitytracker.com/alerts/2009/Dec/1023293.html

CVE Reference:

CVE-2009-3673 (cve.mitre.org, nvd.nist.gov)

• 18624 Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability (CVE-2009-3674) (MS09-072/976325) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. 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. 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.

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

References:

* MS: MS09-072
http://www.microsoft.com/technet/security/bulletin/ms09-072.mspx
* BID: 37213
http://www.securityfocus.com/bid/37213
* VUPEN: VUPEN/ADV-2009-3437
http://www.vupen.com/english/advisories/2009/3437
* SECTRACK: 1023293
http://securitytracker.com/alerts/2009/Dec/1023293.html

CVE Reference:

CVE-2009-3674 (cve.mitre.org, nvd.nist.gov)

- **18625 Internet Authentication Service Memory Corruption Vulnerability (MS09-071/974318) (Remote File Checking)**

A remote code execution vulnerability exists in implementations of Protected Extensible Authentication Protocol (PEAP) on the Internet Authentication Service. The vulnerability is due to incorrect copying into memory of messages received by the server when handling PEAP authentication attempts. 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:

* MS: MS09-071
http://www.microsoft.com/technet/security/bulletin/MS09-071.mspx
* BID: 37197
http://www.securityfocus.com/bid/37197
* VUPEN: VUPEN/ADV-2009-3436
http://www.vupen.com/english/advisories/2009/3436
* SECTRACK: 1023291
http://securitytracker.com/alerts/2009/Dec/1023291.html

CVE Reference:

CVE-2009-2505 (cve.mitre.org, nvd.nist.gov)

- **18626 MS-CHAP Authentication Bypass Vulnerability (MS09-071/974318) (Remote File Checking)**

An elevation of privilege vulnerability exists in the Internet Authentication Service. An attacker could send a specially crafted Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) authentication request that could obtain access to network resources under the privileges of a specific, authorized user.

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

References:

* MS: MS09-071
http://www.microsoft.com/technet/security/bulletin/MS09-071.mspx
* BID: 37198
http://www.securityfocus.com/bid/37198
* VUPEN: VUPEN/ADV-2009-3435
http://www.vupen.com/english/advisories/2009/3435
* SECTRACK: 1023291
http://securitytracker.com/alerts/2009/Dec/1023291.html

CVE Reference:

CVE-2009-3677 (cve.mitre.org, nvd.nist.gov)

- **18627 Single Sign On Spoofing in ADFS Vulnerability (MS09-070/971726) (Remote File Checking)**

A spoofing vulnerability in Active Directory Federation Services could allow an attacker to impersonate an authenticated user if the attacker has access to a workstation and Web browser recently used by the targeted user to access a Web site that offers single sign on.

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

References:

* MS: MS09-070
http://www.microsoft.com/technet/security/bulletin/MS09-070.mspx
* BID: 37215
http://www.securityfocus.com/bid/37215
* VUPEN: VUPEN/ADV-2009-3434
http://www.vupen.com/english/advisories/2009/3434
* SECTRACK: 1023296
http://securitytracker.com/alerts/2009/Dec/1023296.html

CVE Reference:

CVE-2009-2508 (cve.mitre.org, nvd.nist.gov)

- **18628 Remote Code Execution in ADFS Vulnerability (MS09-070/971726) (Remote File Checking)**

A remote code execution vulnerability exists in implementations of Active Directory Federation Services (ADFS). The vulnerability is due to incorrect validation of request headers when an authenticated user connects to an ADFS enabled Web server. 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:

* MS: MS09-070
http://www.microsoft.com/technet/security/bulletin/MS09-070.mspx
* BID: 37214
http://www.securityfocus.com/bid/37214
* VUPEN: VUPEN/ADV-2009-3434
http://www.vupen.com/english/advisories/2009/3434
* SECTRACK: 1023296
http://securitytracker.com/alerts/2009/Dec/1023296.html

CVE Reference:

CVE-2009-2509 (cve.mitre.org, nvd.nist.gov)

- **18629 Local Security Authority Subsystem Service Resource Exhaustion Vulnerability (MS09-069/974392) (Remote File Checking)**

A denial of service vulnerability exists in Microsoft Windows due to the way that the Local Security Authority Subsystem Service (LSASS) improperly handles specially crafted ISAKMP messages communicated through IPsec.

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

References:

* MS: MS09-069
http://www.microsoft.com/technet/security/bulletin/MS09-069.mspx
* BID: 37218
http://www.securityfocus.com/bid/37218
* VUPEN: VUPEN/ADV-2009-3433
http://www.vupen.com/english/advisories/2009/3433
* SECTRACK: 1023297
http://securitytracker.com/alerts/2009/Dec/1023297.html

CVE Reference:

CVE-2009-3675 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2009-2505 Microsoft CVSS 2.0 Score = 10.0**

The Internet Authentication Service (IAS) in Microsoft Windows Vista SP2 and Server 2008 SP2 does not properly validate MS-CHAP v2 Protected Extensible Authentication Protocol (PEAP) authentication requests, which allows remote attackers to execute arbitrary code via crafted structures in a malformed request, aka "Internet Authentication Service Memory Corruption Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-071.mspx

CVE Reference: CVE-2009-2505

- **CVE-2009-3677 Microsoft CVSS 2.0 Score = 10.0**

The Internet Authentication Service (IAS) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold and SP1, and Server 2008 Gold does not properly verify the credentials in an MS-CHAP v2 Protected Extensible Authentication Protocol (PEAP) authentication request, which allows remote attackers to access network resources via a malformed request, aka "MS-CHAP Authentication Bypass Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-071.mspx

CVE Reference: CVE-2009-3677

- **CVE-2009-0102 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Project 2000 SR1 and 2002 SP1, and Office Project 2003 SP3, does not properly handle memory allocation for Project files, which allows remote attackers to execute arbitrary code via a malformed file, aka "Project Memory Validation Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-074.mspx

CVE Reference: CVE-2009-0102

- **CVE-2009-2506 Microsoft CVSS 2.0 Score = 9.3**

The text converters in Microsoft Office Word 2002 SP3 and 2003 SP3; Works 8.5; Office Converter Pack; and WordPad in Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 do not properly parse Word 97 documents, which allows remote attackers to execute arbitrary code via a crafted document, aka "WordPad and Office Text converter Memory Corruption Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-073.mspx

CVE Reference: CVE-2009-2506

- **CVE-2009-3671 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 8 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "Uninitialized Memory Corruption Vulnerability," a different vulnerability than CVE-2009-3674.

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-072.mspx

CVE Reference: CVE-2009-3671

- **CVE-2009-3673 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 7 and 8 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "Uninitialized Memory Corruption Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-072.mspx

CVE Reference: CVE-2009-3673

- **CVE-2009-3674 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 8 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "Uninitialized Memory Corruption Vulnerability," a different vulnerability than CVE-2009-3671.

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-072.mspx

CVE Reference: CVE-2009-3674

- **CVE-2009-2509 Microsoft CVSS 2.0 Score = 9.0**

Active Directory Federation Services (ADFS) in Microsoft Windows Server 2003 SP2 and Server 2008 Gold and SP2 does not properly validate headers in HTTP requests, which allows remote authenticated users to execute arbitrary code via a crafted request to an IIS web server, aka "Remote Code Execution in ADFS Vulnerability."

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

References:

MS: http://www.microsoft.com/technet/security/Bulletin/MS09-070.mspx

CVE Reference: CVE-2009-2509

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