

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

[Apache Chunked Vulnerability Scanner](#) - The S4 Apache Chunked 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 Apache Chunked Encoding buffer overflow.

Download Here:

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

This Week in Review

It is time for plans against threats. Companies should plan how to handle a breach. Cloud security with virtualization technology. Cyberattack on Canada from China.

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

• RSA: Act now on cyberwar, security experts caution

Computerworld - SAN FRANCISCO -- The time to act on cyberwar is now, several experts at the RSA Security Conference held here this week said.

Disagreements may persist on what constitutes an overt act of cyberwar or how to recognize such an act, they admitted. And questions also remain on whether cyberwar is an accurate term to describe deliberate attacks against critical infrastructure targets by enemies that may or may not be state-sponsored.

Even so, the time has arrived for the U.S. to develop a strategic plan for dealing with threats against critical infrastructure and those targeting U.S. economic interests, they said. Computerworld

Full Story :

http://www.computerworld.com/s/article/9209980/RSA_Act_now_on_cyberwar_security_experts_caution?source=rss

• Attack mitigation tools fall short, security vendors say

Computerworld - SAN FRANCISCO -- Acknowledging that security technologies to prevent cyberattacks aren't always up to the task, several vendors at the RSA Conference here advised companies that are making security plans to just assume that they will be breached at some point.

Rather than pouring resources into stopping all attacks, the better strategy is to acknowledge that some attacks will inevitably penetrate their defenses, they said. Therefore, the goal of any enterprise security strategy is not to focus solely on attack mitigation, but also on quick detection and response.

"The typical focus today is on trying to prevent malware from getting in through the front door," said Bret Hartman, chief technology officer at RSA, the security division of EMC. "The problem with that approach is that there's always a percentage [of malware] that does make it through. There's been an overemphasis on infiltration. The goal is to shift focus and assume that you have been infiltrated." Computerworld

Full Story :

http://www.computerworld.com/s/article/9209719/Attack_mitigation_tools_fall_short_security_vendors_say?source=

• **Virtualization can be key to cloud security, RSA chief says**

Computerworld - SAN FRANCISCO -- Virtualization technologies can help enable better security and control in cloud computing environments, RSA chief Art Coviello said today.

In a keynote address at the RSA Security Conference here, Coviello struck an optimistic tone on cloud security issues. While he acknowledged some of the concerns enterprises might have about moving data and applications to the cloud, he said that approaches to addressing any issues are closer than many think.

"Trust in the cloud is achievable today," Coviello said, adding that the key is to stop depending on security controls designed for physical infrastructures. Instead, companies need to be thinking about leveraging virtualization technologies to enable the enhanced security, visibility and control they want in cloud environments. Computerworld

Full Story :

http://www.computerworld.com/s/article/9209578/Virtualization_can_be_key_to_cloud_security_RSA_chief_says?so

• **Report: Canadian cyberattack traced to China**

A cyberattack against Canada that tried to access classified government information and forced two key departments to go offline has been traced back to China, according to a story today from CBC News.

Sources told the CBC that the attacks were initially discovered in early January but that it's unknown whether the attackers themselves were in China or just directed their attacks through the country to hide their true source.

Specifically, the attacks reached computer systems at the Canadian government's Finance Department and Treasury Board in an attempt to capture passwords for government databases. In response, the government was forced to shut down all Internet access for the two departments, according to the CBC, and only now are public employees slowly getting that access back. Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20032813-83.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• **19192 IIS FTP Service Heap Buffer Overrun Vulnerability (MS11-004/2489256) (Remote File Checking)**

A vulnerability exists in the FTP Service in Microsoft Internet Information Services (IIS) 7.0 and Microsoft Internet Information Services (IIS) 7.5. The vulnerability could allow remote code execution.

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

References:

* SECTRACK: 1024921

<http://www.securitytracker.com/id/1024921>

* MS: MS11-004

<http://www.microsoft.com/technet/security/Bulletin/MS11-004.msp>

* EXPLOIT-DB: 15803

<http://www.exploit-db.com/exploits/15803>

* MISC:

<http://blogs.technet.com/b/srd/archive/2011/01/07/assessing-the-risk-of-public-issues-currently-being-tracked-by-the-msrc>

* CERT-VN: VU#842372

<http://www.kb.cert.org/vuls/id/842372>

* BID: 45542
<http://www.securityfocus.com/bid/45542>
* SECTRACK: 1024921
<http://www.securitytracker.com/id?1024921>
* SECUNIA: 42713
<http://secunia.com/advisories/42713>
* VUPEN: ADV-2010-3305
<http://www.vupen.com/english/advisories/2010/3305>
* XF: ms-iis-onsenddata-bo(64248)
<http://xforce.iss.net/xforce/xfdb/64248>

CVE Reference:

CVE-2010-3972 (cve.mitre.org, nvd.nist.gov)

• 19198 Driver Improper Interaction with Windows Kernel Vulnerability (MS11-011/2393802) (Remote File Checking)

An elevation of privilege vulnerability exists due to the improper interaction of drivers with the Windows kernel. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode 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 administrative rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* EXPLOIT-DB: 15609
<http://www.exploit-db.com/exploits/15609/>
* MISC:
<http://isc.sans.edu/diary.html?storyid=9988>
* MISC:
<http://nakedsecurity.sophos.com/2010/11/25/new-windows-zero-day-flaw-bypasses-uac/>
* MISC:
<http://twitter.com/msftsecresponse/statuses/7590788200402945>
* MISC:
<http://www.exploit-db.com/bypassing-uac-with-user-privilege-under-windows-vista7-mirror/>
* CONFIRM:
<http://support.avaya.com/css/P8/documents/100127248>
* MS: MS11-011
<http://www.microsoft.com/technet/security/Bulletin/MS11-011.mspx>
* CERT-VN: VU#529673
<http://www.kb.cert.org/vuls/id/529673>
* BID: 45045
<http://www.securityfocus.com/bid/45045>
* SECTRACK: 1025046
<http://www.securitytracker.com/id?1025046>
* SECUNIA: 42356
<http://secunia.com/advisories/42356>
* VUPEN: ADV-2011-0324
<http://www.vupen.com/english/advisories/2011/0324>

CVE Reference:

CVE-2010-4398 (cve.mitre.org, nvd.nist.gov)

• 19199 Windows Kernel Integer Truncation Vulnerability (MS11-011/2393802) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that the Windows kernel allocates memory when reading user-supplied data. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode 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 administrative rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* BUGTRAQ: 20110208 ZDI-11-064: Microsoft Windows WmiTraceMessageVa Local Kernel Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/516276/100/0/threaded>
* MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-11-064>
* CONFIRM:

<http://support.avaya.com/css/P8/documents/100127248>

* MS: MS11-011

<http://www.microsoft.com/technet/security/Bulletin/MS11-011.msp>

* BID: 46136

<http://www.securityfocus.com/bid/46136>

* OSVDB: 70823

<http://osvdb.org/70823>

* SECTRACK: 1025046

<http://www.securitytracker.com/id?1025046>

* VUPEN: ADV-2011-0324

<http://www.vupen.com/english/advisories/2011/0324>

* XF: ms-win-kernel-privilege-escalation(64926)

<http://xforce.iss.net/xforce/xfdb/64926>

CVE Reference:

CVE-2011-0045 (cve.mitre.org, nvd.nist.gov)

• 19200 Visio Object Memory Corruption Vulnerability (MS11-008/2451879) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Visio validates objects in memory when parsing specially crafted Visio files. 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 / Gain Root** Risk: **High**

References:

* BUGTRAQ: 20110208 ZDI-11-063: Microsoft Visio 2007 LZW Stream Decompression Exception Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/516274/100/0/threaded>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-11-063/>

* MS: MS11-008

<http://www.microsoft.com/technet/security/Bulletin/MS11-008.msp>

* BID: 46137

<http://www.securityfocus.com/bid/46137>

* OSVDB: 70828

<http://osvdb.org/70828>

* SECTRACK: 1025043

<http://www.securitytracker.com/id?1025043>

* SECUNIA: 43254

<http://secunia.com/advisories/43254>

* VUPEN: ADV-2011-0321

<http://www.vupen.com/english/advisories/2011/0321>

* XF: ms-visio-object-code-execution(64923)

<http://xforce.iss.net/xforce/xfdb/64923>

CVE Reference:

CVE-2011-0092 (cve.mitre.org, nvd.nist.gov)

• 19201 Visio Data Type Memory Corruption Vulnerability (MS11-008/2451879) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Visio parses certain structures when handling specially crafted Visio files. 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 / Gain Root** Risk: **High**

References:

* MS: MS11-008

<http://www.microsoft.com/technet/security/Bulletin/MS11-008.msp>

* BID: 46138

<http://www.securityfocus.com/bid/46138>

* OSVDB: 70829

<http://osvdb.org/70829>

* SECTRACK: 1025043

<http://www.securitytracker.com/id?1025043>

* SECUNIA: 43254

<http://secunia.com/advisories/43254>

* VUPEN: ADV-2011-0321

<http://www.vupen.com/english/advisories/2011/0321>

* XF: ms-visio-data-code-execution(64924)

<http://xforce.iss.net/xforce/xfdb/64924>

CVE Reference:

CVE-2011-0093 (cve.mitre.org, nvd.nist.gov)

• 19202 Kerberos Unkeyed Checksum Vulnerability (MS11-013/2496930) (Remote File Checking)

An elevation of privilege vulnerability exists in implementations of Kerberos. The vulnerability exists because the Microsoft Kerberos implementation supports a weak hashing mechanism, which can allow for certain aspects of a Kerberos service ticket to be forged. A malicious user or attacker who successfully exploited this vulnerability could obtain a token with elevated privileges on the affected system.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100127250>

* MS: MS11-013

<http://www.microsoft.com/technet/security/Bulletin/MS11-013.msp>

* BID: 46130

<http://www.securityfocus.com/bid/46130>

* OSVDB: 70834

<http://osvdb.org/70834>

* SECTRACK: 1025048

<http://www.securitytracker.com/id?1025048>

* SECUNIA: 43251

<http://secunia.com/advisories/43251>

* VUPEN: ADV-2011-0326

<http://www.vupen.com/english/advisories/2011/0326>

* XF: ms-kerberos-checksum-privilege-escalation(64900)

<http://xforce.iss.net/xforce/xfdb/64900>

CVE Reference:

CVE-2011-0043 (cve.mitre.org, nvd.nist.gov)

• 19203 Kerberos Spoofing Vulnerability (MS11-013/2496930) (Remote File Checking)

A spoofing vulnerability exists in implementations of Kerberos on Windows 7 and Windows Server 2008 R2. The vulnerability exists because it is possible to downgrade Kerberos authentication to use DES instead of the default, stronger encryption standards included in Windows 7 and Windows Server 2008 R2.

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

References:

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100127250>

* MS: MS11-013

<http://www.microsoft.com/technet/security/Bulletin/MS11-013.msp>

* BID: 46140

<http://www.securityfocus.com/bid/46140>

* OSVDB: 70835

<http://osvdb.org/70835>

* SECTRACK: 1025048

<http://www.securitytracker.com/id?1025048>

* SECUNIA: 43257

<http://secunia.com/advisories/43257>

* VUPEN: ADV-2011-0326

<http://www.vupen.com/english/advisories/2011/0326>

* XF: ms-kerberos-spoofing(64901)

<http://xforce.iss.net/xforce/xfdb/64901>

CVE Reference:

CVE-2011-0091 (cve.mitre.org, nvd.nist.gov)

• 19204 CSRSS Elevation of Privilege Vulnerability (MS11-010/2476687) (Remote File Checking)

An elevation of privilege vulnerability exists in the way that the Windows Client/Server Run-time Subsystem (CSRSS) terminates a process when a user logs off. An attacker who successfully exploited this vulnerability could run code designed to monitor the actions of a user who subsequently logged on to the system. This could allow the disclosure of sensitive information or access to data on the affected systems that was accessible to the logged-on user. This sensitive data could include the logon credentials of subsequent users, which an attacker might later use for elevation of privilege or to execute code as a different user on the system. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly. It could be used to collect useful information to try to further compromise the affected system. If a user with administrative privileges subsequently logs on to the system, the attacker could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights.

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

References:

- * MS: MS11-010
<http://www.microsoft.com/technet/security/Bulletin/MS11-010.mspx>
- * OSVDB: 70826
<http://osvdb.org/70826>
- * SECTRACK: 1025045
<http://www.securitytracker.com/id?1025045>
- * SECUNIA: 43250
<http://secunia.com/advisories/43250>
- * VUPEN: ADV-2011-0323
<http://www.vupen.com/english/advisories/2011/0323>
- * XF: ms-csrss-privilege-escalation(64917)
<http://xforce.iss.net/xforce/xfdb/64917>

CVE Reference:

CVE-2011-0030 (cve.mitre.org, nvd.nist.gov)

• 19205 LSASS Length Validation Vulnerability (MS11-014/2478960) (Remote File Checking)

An elevation of privilege vulnerability exists in the way that the Microsoft Windows Local Security Authority Subsystem Service (LSASS) processes specially crafted authentication requests. The vulnerability could allow an attacker to run code with elevated privileges. 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 administrative rights.

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

References:

- * MS: MS11-014
<http://www.microsoft.com/technet/security/Bulletin/MS11-014.mspx>
- * BID: 46152
<http://www.securityfocus.com/bid/46152>
- * SECTRACK: 1025049
<http://www.securitytracker.com/id?1025049>
- * SECUNIA: 43253
<http://secunia.com/advisories/43253>
- * VUPEN: ADV-2011-0327
<http://www.vupen.com/english/advisories/2011/0327>

CVE Reference:

CVE-2011-0039 (cve.mitre.org, nvd.nist.gov)

• 19206 Active Directory SPN Validation Vulnerability (MS11-005/2478953) (Remote File Checking)

A denial of service vulnerability exists in implementations of Microsoft Windows Active Directory due to improper validation of service principal names (SPN), which could result in SPN collisions. When this occurs, services that use the SPN will downgrade to NT LAN Manager (NTLM) if configured to negotiate. Services that are not configured to negotiate will become unavailable, resulting in a denial of service condition. An attacker who successfully exploited this vulnerability could cause the affected system to stop responding.

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

References:

* MS: MS11-005
<http://www.microsoft.com/technet/security/Bulletin/MS11-005.msp>
* BID: 46145
<http://www.securityfocus.com/bid/46145>
* OSVDB: 70825
<http://osvdb.org/70825>
* SECTRACK: 1025042
<http://www.securitytracker.com/id?1025042>
* SECUNIA: 43215
<http://secunia.com/advisories/43215>
* VUPEN: ADV-2011-0319
<http://www.vupen.com/english/advisories/2011/0319>
* XF: ms-win-active-directory-dos(64915)
<http://xforce.iss.net/xforce/xfdb/64915>

CVE Reference:

CVE-2011-0040 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2011-0654 Microsoft CVSS 2.0 Score = 10.0**

Heap-based buffer overflow in Mrxsmb.sys in Microsoft Windows Server 2003 Active Directory allows remote attackers to execute arbitrary code via a crafted BROWSER ELECTION request.

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

References:

BID: <http://www.securityfocus.com/bid/46360>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/16166>

FULLDISC: <http://archives.neohapsis.com/archives/fulldisclosure/current/0284.html>

CVE Reference: [CVE-2011-0654](http://cve.mitre.org/cve/2011/0654)

• **CVE-2011-1033 IBM CVSS 2.0 Score = 9.3**

Stack-based buffer overflow in oninit in IBM Informix Dynamic Server (IDS) 11.50 allows remote attackers to execute arbitrary code via crafted arguments in the USELASTCOMMITTED session environment option in a SQL SET ENVIRONMENT statement.

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

References:

MISC: <http://zerodayinitiative.com/advisories/ZDI-11-050/>

XF: <http://xforce.iss.net/xforce/xfdb/65209>

VUPEN: <http://www.vupen.com/english/advisories/2011/0309>

BID: <http://www.securityfocus.com/bid/46230>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/516250/100/0/threaded>

SECUNIA: <http://secunia.com/advisories/43212>

MISC: <http://dvlabs.tippingpoint.com/blog/2011/02/07/zdi-disclosure-ibm>

CVE Reference: [CVE-2011-1033](http://cve.mitre.org/cve/2011/1033)

• **CVE-2011-1032 IBM CVSS 2.0 Score = 6.8**

IBM Lotus Connections 3.0, when IBM WebSphere Application Server 7.0.0.11 is used, does not properly restrict access to the internal login module, which has unspecified impact and attack vectors.

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

References:

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg21462435>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PK54565>

SECUNIA: <http://secunia.com/advisories/43298>

CVE Reference: [CVE-2011-1032](#)

• **CVE-2011-1030 IBM CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in the Wikis component in IBM Lotus Connections 3.0 allows remote attackers to inject arbitrary web script or HTML via vectors related to the "Confirm New Page scene."

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

References:

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=swg1LO57850>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?crawler=1&uid=swg1LO57850>

SECTRAK: <http://securitytracker.com/id?1025054>

SECUNIA: <http://secunia.com/advisories/43134>

CVE Reference: [CVE-2011-1030](#)

• **CVE-2008-7274 IBM CVSS 2.0 Score = 4.3**

IBM WebSphere Application Server (WAS) 6.1.0.9, when the JAAS Login functionality is enabled, allows attackers to perform an internal application hashtable login by (1) not providing a password or (2) providing an empty password.

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

References:

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg1PK54565>

CVE Reference: [CVE-2008-7274](#)

• **CVE-2011-1034 IBM CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in the UI in IBM Rational Build Forge 7.0.2 allows remote attackers to inject arbitrary web script or HTML via the mod parameter to the fullcontrol program. NOTE: some of these details are obtained from third party information.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2011/0276>

BID: <http://www.securityfocus.com/bid/46125>

OSVDB: <http://www.osvdb.org/70763>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=swg1PM05187>

SECTRAK: <http://securitytracker.com/id?1025019>

SECUNIA: <http://secunia.com/advisories/43180>

CVE Reference: [CVE-2011-1034](#)

• **CVE-2011-1029 IBM CVSS 2.0 Score = 3.5**

Cross-site scripting (XSS) vulnerability in IBM Rational Team Concert (RTC) 2.0.0.x allows remote authenticated users to inject arbitrary web script or HTML via the name of a shared report.

Test Case Impact: Vulnerability Impact: Risk: **Low**

References:

XF: <http://xforce.iss.net/xforce/xfdb/65170>

VUPEN: <http://www.vupen.com/english/advisories/2011/0297>

BID: <http://www.securityfocus.com/bid/46179>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=swg1PM22477>

SECUNIA: <http://secunia.com/advisories/43223>

CVE Reference: [CVE-2011-1029](#)

• **CVE-2011-0355 Cisco CVSS 2.0 Score = 7.8**

Cisco Nexus 1000V Virtual Ethernet Module (VEM) 4.0(4) SV1(1) through SV1(3b), as used in VMware ESX 4.0 and 4.1 and ESXi 4.0 and 4.1, does not properly handle dropped packets, which allows guest OS users to cause a denial of service (ESX or ESXi host OS crash) by sending an 802.1Q tagged packet over an access vEthernet port, aka Cisco Bug ID CSCtj17451.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/65217>

VUPEN: <http://www.vupen.com/english/advisories/2011/0315>

VUPEN: <http://www.vupen.com/english/advisories/2011/0314>

CONFIRM: <http://www.vmware.com/security/advisories/VMSA-2011-0002.html>

BID: <http://www.securityfocus.com/bid/46247>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/516259/100/0/threaded>

OSVDB: <http://www.osvdb.org/70837>

CONFIRM:

http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_sv1_3_c/release/notes/n1000v_rn.html

SECTRACK: <http://securitytracker.com/id?1025030>

SECUNIA: <http://secunia.com/advisories/43084>

MLIST: <http://lists.vmware.com/pipermail/security-announce/2011/000118.html>

CVE Reference: [CVE-2011-0355](#)

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