

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, netVigilance - the SC Magazine vulnerability assessment Innovator Dec 2010, implemented a series of major performance enhancements to the core of our technology:

(1) 10% reduction (on average) of the already low bandwidth traffic between the main console and the remote scanning agents.

(2) Major overhaul to our propriety caching technology and optimized connectivity checking gives a 25% improvement in both execution speed and bandwidth requirements.

(3) Fixed issue resulting in inaccurate progress calculation, so now when the scan progress reaches 100% the scan really is finished.

From the news: Call for obligation to reveal breeches. The insider threat - Today. Should companies not ban use of own equipment? Warning about vulnerable critical infrastructure management systems.

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

• **Senators call on SEC to mandate more breach reporting**

Prompted by recent breaches of intellectual property belonging to U.S. corporations, federal lawmakers want the Securities and Exchange Commission (SEC) to clarify guidance around the obligation to publicly disclose these incidents to shareholders.

In a Wednesday letter to SEC Chairwoman Mary Schapiro, five senators said existing securities regulations require publicly traded businesses to reveal any "material network breach." That includes incidents leading to the loss of sensitive data, such as intellectual property and trade secrets, which could be used by adversaries to gain a competitive advantage, impact earnings or shrink market share.

Judy Burns, an SEC spokeswoman, said the agency hasn't specifically issued guidance related to breaches, but such incidents likely are covered under securities laws from the 1930s. SC Magazine

Full Story :

http://www.scmagazineus.com/senators-call-on-sec-to-mandate-more-breach-reporting/article/202689/?utm_source=

• **The 3 types of insider threat**

CSO - Why does your competitor have your latest research or financial figures? It must be an insider -- or is it?

Before the digital revolution, security professionals were kept awake at night worrying about the potential threat posed by an untrustworthy member of their organization. Commonly referred to as the "insider threat," this person possibly had privileged access to classified, sensitive or propriety data; providing the insider a unique opportunity, given his or her capabilities, to remove information, predominately in paper form, from the facility and transfer it to whomever they desired.

See also: Are you an insider threat? Computerworld

Full Story :

http://www.computerworld.com/s/article/9216652/The_3_types_of_insider_threat?source=rss_security&utm_source=

• **Banning consumer devices makes a firm less secure**

CSO - I was having a conversation with another fellow security professional at the CSO Perspectives seminar a few weeks ago and he used the word "disintermediation" to make a point about his website. We had a bit of a chuckle about how that word that was used (rather, overused) during the dot-com days. The context back then was that the new, online world was going to obsolesce the traditional world of bricks-n-mortars through the "disintermediation" process of cutting out the no-value-adding, costly infrastructure of middle-men.

This got me to thinking about the topic I was speaking about at the conference: the way to bring about a culturally acceptable balance between security and the use of consumerized IT. That is, how could IT departments allow users to bring and use their own equipment in the work environment and still maintain a modicum of security and privacy?

Also see: How to adopt consumer tech for efficiency Computerworld

Full Story :

http://www.computerworld.com/s/article/9216605/Banning_consumer_devices_makes_a_firm_less_secure?source=

• **Industrial control systems at risk, ICS-CERT warns**

Two popular software products used to manage critical infrastructure facilities contain a vulnerability that could allow an attacker to take control of affected systems, the U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) warned Wednesday. The affected products, Genesis32 and BizViz, both web-based supervisory control and data acquisition (SCADA) systems manufactured by U.S.-based Iconics, contain a vulnerability that could be exploited by an attacker to execute arbitrary code on an affected system, ICS-CERT said. The products are used to manage manufacturing, building automation, oil, gas, water and electric facilities in the United States, Europe and Asia.

Security researchers from Security-Assessment.com, a New Zealand-based penetration testing and vulnerability assessment firm, discovered the flaw - a stack overflow vulnerability affecting an ActiveX control incorporated in both products. SC Magazine

Full Story :

http://www.scmagazineus.com/industrial-control-systems-at-risk-ics-cert-warns/article/202673/?utm_source=feedburn

New Vulnerabilities Tested in SecureScout

• 19320 Win32k Use After Free Vulnerability (CVE-2011-1241) (MS11-034/2506223) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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 / Gain Root** Risk: **High**

References:

* MISC:

<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100133352>

* MS: MS11-034

<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>

* BID: 47218

<http://www.securityfocus.com/bid/47218>

* OSVDB: 71756

<http://osvdb.org/71756>

* SECTRACK: 1025345

<http://www.securitytracker.com/id?1025345>

* SECUNIA: 44156

<http://secunia.com/advisories/44156>

* VUPEN: ADV-2011-0952

<http://www.vupen.com/english/advisories/2011/0952>

CVE Reference:

CVE-2011-1241 (cve.mitre.org, nvd.nist.gov)

• 19321 Win32k Use After Free Vulnerability (CVE-2011-1242) (MS11-034/2506223) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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 / Gain Root** Risk: **High**

References:

* MISC:

<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100133352>

* MS: MS11-034

<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>

* BID: 47219

<http://www.securityfocus.com/bid/47219>

* OSVDB: 71757

<http://osvdb.org/71757>

* SECTRACK: 1025345

<http://www.securitytracker.com/id?1025345>

* SECUNIA: 44156

<http://secunia.com/advisories/44156>

* VUPEN: ADV-2011-0952

<http://www.vupen.com/english/advisories/2011/0952>

CVE Reference:

CVE-2011-1242 (cve.mitre.org, nvd.nist.gov)

• 19322 Win32k Null Pointer De-reference Vulnerability (CVE-2011-0673) (MS11-034/2506223) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage pointers to kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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 / Gain Root** Risk: **High**

References:

* MISC:

<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100133352>

* MS: MS11-034

<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>

* BID: 47234

<http://www.securityfocus.com/bid/47234>

* SECTRACK: 1025345

<http://www.securitytracker.com/id?1025345>

* SECUNIA: 44156

<http://secunia.com/advisories/44156>

* VUPEN: ADV-2011-0952

<http://www.vupen.com/english/advisories/2011/0952>

* XF: mswin-win32k-var8-priv-escalation(66402)

<http://xforce.iss.net/xforce/xfdb/66402>

CVE Reference:

CVE-2011-0673 (cve.mitre.org, nvd.nist.gov)

• 19323 Win32k Null Pointer De-reference Vulnerability (CVE-2011-0676) (MS11-034/2506223) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage pointers to kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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 / Gain Root** Risk: **High**

References:

* MISC:

<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100133352>

* MS: MS11-034

<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>

* BID: 47220

<http://www.securityfocus.com/bid/47220>

* SECTRACK: 1025345

<http://www.securitytracker.com/id?1025345>

* SECUNIA: 44156

<http://secunia.com/advisories/44156>

* VUPEN: ADV-2011-0952

<http://www.vupen.com/english/advisories/2011/0952>

* XF: mswin-win32k-var11-priv-escalation(66405)

<http://xforce.iss.net/xforce/xfdb/66405>

CVE Reference:

CVE-2011-0676 (cve.mitre.org, nvd.nist.gov)

• 19324 Win32k Null Pointer De-reference Vulnerability (CVE-2011-0677) (MS11-034/2506223) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage pointers to kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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 / Gain Root** Risk: **High**

References:

* MISC:

<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100133352>

* MS: MS11-034

<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>

* BID: 47224
<http://www.securityfocus.com/bid/47224>
* SECTRACK: 1025345
<http://www.securitytracker.com/id?1025345>
* SECUNIA: 44156
<http://secunia.com/advisories/44156>
* VUPEN: ADV-2011-0952
<http://www.vupen.com/english/advisories/2011/0952>
* XF: mswin-win32k-var12-priv-escalation(66406)
<http://xforce.iss.net/xforce/xfdb/66406>

CVE Reference:

CVE-2011-0677 (cve.mitre.org, nvd.nist.gov)

• **19325 Win32k Null Pointer De-reference Vulnerability (CVE-2011-1225) (MS11-034/2506223) (Remote File Checking)**

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage pointers to kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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 / Gain Root** Risk: **High**

References:

* MISC:
<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>
* CONFIRM:
<http://support.avaya.com/css/P8/documents/100133352>
* MS: MS11-034
<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>
* BID: 47225
<http://www.securityfocus.com/bid/47225>
* SECTRACK: 1025345
<http://www.securitytracker.com/id?1025345>
* SECUNIA: 44156
<http://secunia.com/advisories/44156>
* VUPEN: ADV-2011-0952
<http://www.vupen.com/english/advisories/2011/0952>
* XF: mswin-win32k-var13-priv-escalation(66407)
<http://xforce.iss.net/xforce/xfdb/66407>

CVE Reference:

CVE-2011-1225 (cve.mitre.org, nvd.nist.gov)

• **19326 Win32k Null Pointer De-reference Vulnerability (CVE-2011-1226) (MS11-034/2506223) (Remote File Checking)**

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage pointers to kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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 / Gain Root** Risk: **High**

References:

* MISC:
<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>
* CONFIRM:
<http://support.avaya.com/css/P8/documents/100133352>
* MS: MS11-034
<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>
* BID: 47226
<http://www.securityfocus.com/bid/47226>
* OSVDB: 71731
<http://osvdb.org/71731>
* SECTRACK: 1025345
<http://www.securitytracker.com/id?1025345>
* SECUNIA: 44156

<http://secunia.com/advisories/44156>

* VUPEN: ADV-2011-0952

<http://www.vupen.com/english/advisories/2011/0952>

* XF: mswin-win32k-var14-priv-escalation(66408)

<http://xforce.iss.net/xforce/xfdb/66408>

CVE Reference:

CVE-2011-1226 (cve.mitre.org, nvd.nist.gov)

• 19327 Win32k Null Pointer De-reference Vulnerability (CVE-2011-1227) (MS11-034/2506223) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage pointers to kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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 / Gain Root** Risk: **High**

References:

* MISC:

<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100133352>

* MS: MS11-034

<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>

* BID: 47227

<http://www.securityfocus.com/bid/47227>

* OSVDB: 71732

<http://osvdb.org/71732>

* SECTRACK: 1025345

<http://www.securitytracker.com/id?1025345>

* SECUNIA: 44156

<http://secunia.com/advisories/44156>

* VUPEN: ADV-2011-0952

<http://www.vupen.com/english/advisories/2011/0952>

* XF: mswin-win32k-var15-priv-escalation(66409)

<http://xforce.iss.net/xforce/xfdb/66409>

CVE Reference:

CVE-2011-1227 (cve.mitre.org, nvd.nist.gov)

• 19328 Win32k Null Pointer De-reference Vulnerability (CVE-2011-1228) (MS11-034/2506223) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage pointers to kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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 / Gain Root** Risk: **High**

References:

* MISC:

<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100133352>

* MS: MS11-034

<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>

* BID: 47228

<http://www.securityfocus.com/bid/47228>

* OSVDB: 71734

<http://osvdb.org/71734>

* SECTRACK: 1025345

<http://www.securitytracker.com/id?1025345>

* SECUNIA: 44156

<http://secunia.com/advisories/44156>

* VUPEN: ADV-2011-0952

<http://www.vupen.com/english/advisories/2011/0952>

* XF: mswin-win32k-var16-priv-escalation(66410)
<http://xforce.iss.net/xforce/xfdb/66410>

CVE Reference:

CVE-2011-1228 (cve.mitre.org, nvd.nist.gov)

• 19329 Win32k Null Pointer De-reference Vulnerability (CVE-2011-1229) (MS11-034/2506223) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way that Windows Kernel-mode drivers manage pointers to kernel-mode driver objects. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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 / Gain Root** Risk: **High**

References:

* MISC:

<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-034-addressing-vulnerabilities-in-the-win32k-subsystem.aspx>

* CONFIRM:

<http://support.avaya.com/css/P8/documents/100133352>

* MS: MS11-034

<http://www.microsoft.com/technet/security/Bulletin/MS11-034.msp>

* BID: 47229

<http://www.securityfocus.com/bid/47229>

* OSVDB: 71735

<http://osvdb.org/71735>

* SECTRAK: 1025345

<http://www.securitytracker.com/id?1025345>

* SECUNIA: 44156

<http://secunia.com/advisories/44156>

* VUPEN: ADV-2011-0952

<http://www.vupen.com/english/advisories/2011/0952>

* XF: mswin-win32k-var17-priv-escalation(66411)

<http://xforce.iss.net/xforce/xfdb/66411>

CVE Reference:

CVE-2011-1229 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-1271 Microsoft CVSS 2.0 Score = 5.1

The JIT compiler in Microsoft .NET Framework before 4 beta 2, when IsJITOptimizerDisabled is false, does not properly handle expressions related to null strings, which allows context-dependent attackers to bypass intended access restrictions in opportunistic circumstances by leveraging a crafted application, as demonstrated by a C# application on the x86 platform.

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

References:

MISC: <http://stackoverflow.com/questions/2135509/bug-only-occurring-when-compile-optimization-enabled/>

CVE Reference: [CVE-2011-1271](http://cve.mitre.org/cve/2011/1271)

• CVE-2011-1735 HP CVSS 2.0 Score = 10.0

Stack-based buffer overflow in Omninet.exe in the Backup Client Service in HP OpenView Storage Data Protector 6.00, 6.10, and 6.11 allows remote attackers to execute arbitrary code via a malformed bm message.

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

References:

MISC: <http://zerodayinitiative.com/advisories/ZDI-11-151/>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02810240>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02810240>

CVE Reference: [CVE-2011-1735](#)

• **CVE-2011-1734 HP CVSS 2.0 Score = 10.0**

Stack-based buffer overflow in Omninet.exe in the Backup Client Service in HP OpenView Storage Data Protector 6.00, 6.10, and 6.11 allows remote attackers to execute arbitrary code via a malformed omniiaputil message.

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

References:

MISC: <http://zerodayinitiative.com/advisories/ZDI-11-150/>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02810240>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02810240>

CVE Reference: [CVE-2011-1734](#)

• **CVE-2011-1733 HP CVSS 2.0 Score = 10.0**

Stack-based buffer overflow in Omninet.exe in the Backup Client Service in HP OpenView Storage Data Protector 6.00, 6.10, and 6.11 allows remote attackers to execute arbitrary code via a malformed HPFGConfig message.

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

References:

MISC: <http://zerodayinitiative.com/advisories/ZDI-11-149/>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02810240>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02810240>

CVE Reference: [CVE-2011-1733](#)

• **CVE-2011-1732 HP CVSS 2.0 Score = 10.0**

Stack-based buffer overflow in Omninet.exe in the Backup Client Service in HP OpenView Storage Data Protector 6.00, 6.10, and 6.11 allows remote attackers to execute arbitrary code via a malformed stutil message.

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

References:

MISC: <http://zerodayinitiative.com/advisories/ZDI-11-148/>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02810240>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02810240>

CVE Reference: [CVE-2011-1732](#)

• **CVE-2011-1731 HP CVSS 2.0 Score = 10.0**

Stack-based buffer overflow in Omninet.exe in the Backup Client Service in HP OpenView Storage Data Protector 6.00, 6.10, and 6.11 allows remote attackers to execute arbitrary code via a malformed EXEC_INTEGUTIL message.

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

References:

MISC: <http://zerodayinitiative.com/advisories/ZDI-11-147/>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02810240>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02810240>

CVE Reference: [CVE-2011-1731](#)

• **CVE-2011-1730 HP CVSS 2.0 Score = 10.0**

Stack-based buffer overflow in Omninet.exe in the Backup Client Service in HP OpenView Storage Data Protector 6.00, 6.10, and 6.11 allows remote attackers to execute arbitrary code via a malformed EXEC_SCRIPT message.

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

References:

MISC: <http://zerodayinitiative.com/advisories/ZDI-11-146/>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02810240>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02810240>

CVE Reference: [CVE-2011-1730](#)

• CVE-2011-1729 HP CVSS 2.0 Score = 10.0

Stack-based buffer overflow in Omninet.exe in the Backup Client Service in HP OpenView Storage Data Protector 6.00, 6.10, and 6.11 allows remote attackers to execute arbitrary code via a malformed GET_FILE message.

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

References:

MISC: <http://zerodayinitiative.com/advisories/ZDI-11-145/>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02810240>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02810240>

CVE Reference: [CVE-2011-1729](#)

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