

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://www2.netvigilance.com/productdownloads?productname=apachechunkedvulnerabilityscanner>

This Week in Review

Data stealing virus on the loose. More exploits happening at Sony. Standards for security vulnerability reporting on the way. US launching website to help small biz against cyber attack.

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

• Mass. agency says virus led to data breach

A virus that infected as many as 1,500 computers in Massachusetts unemployment offices may have allowed criminals to steal Social Security numbers and other data of individuals and businesses, a state agency warned today.

The W32.QAKBOT data-stealing virus infected the computers on the network of the Department of Unemployment Assistance and Career Services, as well as computers at One Stop Career Centers, according to a statement from the Massachusetts Labor and Workforce Development agency.

It's unclear how many individuals and employers might be affected. The virus only affects people who had their files manually accessed and employers who manually filed their quarterly statements at an infected computer between April 19 and May 13, the agency said. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20063712-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• Sony takes sites down after log-in exploit found

The sign-in for PlayStation Network on the Web was out of service this morning.

(Credit: Screenshot by Erica Ogg/CNET)

Just days after most services for PlayStation Network were brought back online, it appears a new exploit has been discovered that allows hackers to change users' passwords with the data stolen during the break-in to the service last month. Cnet Security

Full Story :

http://news.cnet.com/8301-31021_3-20063973-260.html?part=rss&subj=news&tag=2547-1_3-0-20

• Standardized vulnerability reporting framework unveiled

The nonprofit Industry Consortium for Advancement of Security on the Internet (ICASI) on Tuesday announced the release of a framework designed to standardize security vulnerability reporting.

The free Common Vulnerability Reporting Framework (CVRF) was created to provide security practitioners and vendors with a common method for the creation, dissemination and consumption of security vulnerability data, Mike Schiffman, chairman of ICASI's CVRF working group and a computer security researcher at Cisco, said during a Tuesday conference call announcing the project.

Historically, no accepted standard for security vulnerability reporting has existed, Schiffman said. Because each vendor uses its own format, security practitioners must manually parse through many ad-hoc bug reports and bulletins to find information that is applicable to their environment, a task that is time consuming and imperfect. SC Magazine

Full Story :

http://www.scmagazineus.com/standardized-vulnerability-reporting-framework-unveiled/article/203072/?utm_source=

• FCC unveils cyber defense website for small businesses

The Federal Communications Commission (FCC) on Monday announced the launch of a new website designed to help small businesses protect against cyberattack.

The site -- fcc.gov/cyberforsmallbiz -- includes links to vendor, nonprofit and government resources, including materials from the National Cyber Security Alliance (NCSA) and a PowerPoint presentation from the National Institute of Standards and Technology.

The site also contains a top 10 list of tips for small businesses. They include training employees, installing patches, limiting access and regularly changing passwords. SC Magazine

Full Story :

http://www.scmagazineus.com/fcc-unveils-cyber-defense-website-for-small-businesses/article/203061/?utm_source=

New Vulnerabilities Tested in SecureScout

• 19330 Win32k Null Pointer De-reference Vulnerability (CVE-2011-1230) (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: 47230

<http://www.securityfocus.com/bid/47230>

* OSVDB: 71736

<http://osvdb.org/71736>

* 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-var18-priv-escalation(66412)

<http://xforce.iss.net/xforce/xfdb/66412>

CVE Reference:

CVE-2011-1230 (cve.mitre.org, nvd.nist.gov)

• 19331 Win32k Null Pointer De-reference Vulnerability (CVE-2011-1231) (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: 47231

<http://www.securityfocus.com/bid/47231>

* OSVDB: 71737

<http://osvdb.org/71737>

* 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-var19-priv-escalation(66413)

<http://xforce.iss.net/xforce/xfdb/66413>

CVE Reference:

CVE-2011-1231 (cve.mitre.org, nvd.nist.gov)

• 19332 Win32k Null Pointer De-reference Vulnerability (CVE-2011-1232) (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: 47232

<http://www.securityfocus.com/bid/47232>

* OSVDB: 71738

<http://osvdb.org/71738>

* 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-var20-priv-escalation(66414)
<http://xforce.iss.net/xforce/xfdb/66414>

CVE Reference:

CVE-2011-1232 (cve.mitre.org, nvd.nist.gov)

• 19333 Win32k Null Pointer De-reference Vulnerability (CVE-2011-1233) (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: 47233
<http://www.securityfocus.com/bid/47233>
* OSVDB: 71739
<http://osvdb.org/71739>
* 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-var21-priv-escalation(66415)
<http://xforce.iss.net/xforce/xfdb/66415>

CVE Reference:

CVE-2011-1233 (cve.mitre.org, nvd.nist.gov)

• 19334 Presentation Memory Corruption RCE Vulnerability (MS11-036/2545814) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft PowerPoint handles specially crafted PowerPoint 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.

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

References:

* MS: MS11-036
<http://www.microsoft.com/technet/security/Bulletin/MS11-036.msp>
* BID: 47700
<http://www.securityfocus.com/bid/47700>
* VUPEN: VUPEN/ADV-2011-1201
<http://www.vupen.com/english/advisories/2011/1201>
* SECTRACK: 1025513
<http://www.securitytracker.com/id/1025513>

CVE Reference:

CVE-2011-1269 (cve.mitre.org, nvd.nist.gov)

• 19335 Presentation Buffer Overrun RCE Vulnerability (MS11-036/2545814) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft PowerPoint handles specially crafted PowerPoint 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.

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

References:

- * BID: 47699
<http://www.securityfocus.com/bid/47699>
- * VUPEN: VUPEN/ADV-2011-1201
<http://www.vupen.com/english/advisories/2011/1201>
- * SECTRACK: 1025513
<http://www.securitytracker.com/id/1025513>
- * MS: MS11-036
<http://www.microsoft.com/technet/security/Bulletin/MS11-036.msp>

CVE Reference:

CVE-2011-1270 (cve.mitre.org, nvd.nist.gov)

● **19336 WINS Service Failed Response Vulnerability (MS11-035/2524426) (Remote File Checking)**

A remote code execution vulnerability exists in the Windows Internet Name Service (WINS) due to insufficient validations for the data structures within specially crafted WINS network packets sent to the WINS service.

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

References:

- * BID: 47730
<http://www.securityfocus.com/bid/47730>
- * VUPEN: VUPEN/ADV-2011-1200
<http://www.vupen.com/english/advisories/2011/1200>
- * SECTRACK: 1025512
<http://www.securitytracker.com/id/1025512>
- * MS: MS11-035
<http://www.microsoft.com/technet/security/Bulletin/MS11-035.msp>

CVE Reference:

CVE-2011-1248 (cve.mitre.org, nvd.nist.gov)

● **19337 .NET Framework Stack Corruption Vulnerability (MS11-028/2484015) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft .NET Framework handles certain function calls. 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: MS11-028
<http://www.microsoft.com/technet/security/Bulletin/MS11-028.msp>
- * BID: 47223
<http://www.securityfocus.com/bid/47223>
- * SECTRACK: 1025331
<http://www.securitytracker.com/id/1025331>
- * VUPEN: VUPEN/ADV-2011-0945
<http://www.vupen.com/english/advisories/2011/0945>

CVE Reference:

CVE-2010-3958 (cve.mitre.org, nvd.nist.gov)

● **19338 GDI+ Integer Overflow Vulnerability (MS11-029/2489979) (Remote File Checking)**

A remote code execution vulnerability exists in the way that GDI+ handles integer calculations. The vulnerability could allow remote code execution if a user opens a specially crafted EMF image file. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts 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:

* BID: 47250
<http://www.securityfocus.com/bid/47250>
* SECTRACK: 1025335
<http://www.securitytracker.com/id/1025335>
* VUPEN: VUPEN/ADV-2011-0946
<http://www.vupen.com/english/advisories/2011/0946>
* MS: MS11-029
<http://www.microsoft.com/technet/security/Bulletin/MS11-029.msp>

CVE Reference:

CVE-2011-0041 (cve.mitre.org, nvd.nist.gov)

• **19339 OpenType Font Stack Overflow Vulnerability (MS11-032/2507618) (Remote File Checking)**

A remote code execution vulnerability exists in the way that the OpenType Font (OTF) driver improperly parses specially crafted OpenType fonts. 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** Risk: **High**

References:

* BID: 47179
<http://www.securityfocus.com/bid/47179>
* SECTRACK: 1025334
<http://www.securitytracker.com/id/1025334>
* VUPEN: VUPEN/ADV-2011-0950
<http://www.vupen.com/english/advisories/2011/0950>
* MS: MS11-032
<http://www.microsoft.com/technet/security/Bulletin/MS11-032.msp>

CVE Reference:

CVE-2011-0034 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2011-0419 Apache CVSS 2.0 Score = 4.3**

Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=703390
CONFIRM: <http://www.apache.org/dist/httpd/Announcement2.2.html>
CONFIRM: <http://www.apache.org/dist/apr/Announcement1.x.html>
CONFIRM: <http://svn.apache.org/viewvc?view=revision&revision=1098799>
CONFIRM: <http://svn.apache.org/viewvc?view=revision&revision=1098188>
CONFIRM: http://svn.apache.org/viewvc/apr/apr/branches/1.4.x/strings/apr_fnmatch.c?r1=731029&r2=1098902
MISC: http://cxib.net/stuff/apache_fnmatch.phps
REDHAT: <http://www.redhat.com/support/errata/RHSA-2011-0507.html>
CONFIRM: <http://www.openbsd.org/cgi-bin/cvsweb/src/lib/libc/gen/fnmatch.c#rev1.15>
MLIST: <http://www.mail-archive.com/dev@apr.apache.org/msg23976.html>

MLIST: <http://www.mail-archive.com/dev@apr.apache.org/msg23961.html>

MLIST: <http://www.mail-archive.com/dev@apr.apache.org/msg23960.html>

CONFIRM: <http://www.apache.org/dist/apr/CHANGES-APR-1.4>

SECTRAK: <http://securitytracker.com/id?1025527>

SREASONRES: http://securityreason.com/achievement_securityalert/98

SECUNIA: <http://secunia.com/advisories/44574>

SECUNIA: <http://secunia.com/advisories/44564>

SECUNIA: <http://secunia.com/advisories/44490>

CONFIRM: http://httpd.apache.org/security/vulnerabilities_22.html

MISC: http://cxib.net/stuff/apr_fnmatch.txts

CONFIRM: <http://cvsweb.netbsd.org/bsdweb.cgi/src/lib/libc/gen/fnmatch.c#rev1.22>

CVE Reference: [CVE-2011-0419](#)

• **CVE-2011-0419 Oracle CVSS 2.0 Score = 4.3**

Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via `*?` sequences in the first argument, as demonstrated by attacks against `mod_autoindex` in `httpd`.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=703390

CONFIRM: <http://www.apache.org/dist/httpd/Announcement2.2.html>

CONFIRM: <http://www.apache.org/dist/apr/Announcement1.x.html>

CONFIRM: <http://svn.apache.org/viewvc?view=revision&revision=1098799>

CONFIRM: <http://svn.apache.org/viewvc?view=revision&revision=1098188>

CONFIRM: http://svn.apache.org/viewvc/apr/apr/branches/1.4.x/strings/apr_fnmatch.c?r1=731029&r2=1098902

MISC: http://cxib.net/stuff/apache_fnmatch.phps

REDHAT: <http://www.redhat.com/support/errata/RHSA-2011-0507.html>

CONFIRM: <http://www.openbsd.org/cgi-bin/cvsweb/src/lib/libc/gen/fnmatch.c#rev1.15>

MLIST: <http://www.mail-archive.com/dev@apr.apache.org/msg23976.html>

MLIST: <http://www.mail-archive.com/dev@apr.apache.org/msg23961.html>

MLIST: <http://www.mail-archive.com/dev@apr.apache.org/msg23960.html>

CONFIRM: <http://www.apache.org/dist/apr/CHANGES-APR-1.4>

SECTRAK: <http://securitytracker.com/id?1025527>

SREASONRES: http://securityreason.com/achievement_securityalert/98

SECUNIA: <http://secunia.com/advisories/44574>

SECUNIA: <http://secunia.com/advisories/44564>

SECUNIA: <http://secunia.com/advisories/44490>

CONFIRM: http://httpd.apache.org/security/vulnerabilities_22.html

MISC: http://cxib.net/stuff/apr_fnmatch.txts

CONFIRM: <http://cvsweb.netbsd.org/bsdweb.cgi/src/lib/libc/gen/fnmatch.c#rev1.22>

CVE Reference: [CVE-2011-0419](#)

• **CVE-2011-1856 HP CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in HP Business Availability Center (BAC) 8.06 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

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

References:

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02823184

HP: http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02823184

SECUNIA: <http://secunia.com/advisories/44569>

CVE Reference: [CVE-2011-1856](#)

• **CVE-2011-2141 IBM CVSS 2.0 Score = 7.5**

SQL injection vulnerability in TMWeb in IBM Datacap Taskmaster Capture 8.0.1 before FP1 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/67452>

BID: <http://www.securityfocus.com/bid/47848>

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg27021511>

SECUNIA: <http://secunia.com/advisories/44553>

CVE Reference: [CVE-2011-2141](#)

• **CVE-2011-2143 IBM CVSS 2.0 Score = 6.8**

IBM Datacap Taskmaster Capture 8.0.1 before FP1, when Windows Authentication is enabled, allows remote attackers to obtain login access by using an incorrect password in conjunction with an account name from a different domain.

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

References:

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg27021511>

CVE Reference: [CVE-2011-2143](#)

• **CVE-2011-2144 IBM CVSS 2.0 Score = 5.0**

The eDocument Conversion Actions implementation in IBM Datacap Taskmaster Capture 8.0.1 FP1 and earlier allows remote attackers to cause a denial of service (batch abort) via a long subject line in an e-mail message that is represented in a .eml file.

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

References:

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg27021511>

CVE Reference: [CVE-2011-2144](#)

• **CVE-2011-2142 IBM CVSS 2.0 Score = 5.0**

The Web Client Service in IBM Datacap Taskmaster Capture 8.0.1 before FP1 requires a cleartext password, which has unspecified impact and attack vectors.

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

References:

CONFIRM: <http://www.ibm.com/support/docview.wss?uid=swg27021511>

CVE Reference: [CVE-2011-2142](#)

• **CVE-2011-0615 Adobe CVSS 2.0 Score = 9.3**

Multiple buffer overflows in Adobe Audition 3.0.1 and earlier allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via crafted data in unspecified fields in the TRKM chunk in an Audition Session (aka .ses) file, related to inconsistent use of character data types.

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

References:

BID: <http://www.securityfocus.com/bid/47838>

MISC: <http://www.coresecurity.com/content/Adobe-Audition-malformed-SES-file>

CONFIRM: <http://www.adobe.com/support/security/bulletins/apsb11-10.html>

CVE Reference: [CVE-2011-0615](#)

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