

## 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

Weak security in third-party apps. Majority of cyber attacks use toolkits. Can a USB cable really be attacked? New job application scam.

Enjoy reading & Stay safe.

**Call or email netVigilance to get an update on SecureScout.**

**(503) 524 5758 or [sales@netvigilance.com](mailto:sales@netvigilance.com)**

## Top Security News Stories this Week

### • Third-party apps remains security weak point

IDG News Service - Microsoft is still burdened with a bad reputation among users for security, although figures show its products are more secure than most on a person's computer, according to new data from the Danish security vendor Secunia.

The number of vulnerabilities in software commonly found on PCs shot up by an astounding 71% between 2009 and 2010, mostly due to problems in third-party applications rather than in the Windows OS or Microsoft apps, said Stefan Frei, research analyst director for Secunia. The company released its annual vulnerability report on Tuesday.

"When we dig deeper we find the main contributor is not vulnerabilities in Microsoft products but vulnerabilities in third-party products," Frei said. "Traditionally we still perceive Microsoft programs and the Microsoft operating system to be the main culprit, the main threat. However, this has changed." Computerworld

Full Story :

[http://www.computerworld.com/s/article/9205399/Third\\_party\\_apps\\_remains\\_security\\_weak\\_point?source=rss\\_secu](http://www.computerworld.com/s/article/9205399/Third_party_apps_remains_security_weak_point?source=rss_secu)

## • Report: Toolkits now used in the majority of cyberattacks

So-called cybercrime attack "toolkits" have over the past few years become more accessible and are now used in the majority of internet attacks, according to a report released Tuesday by Symantec. Also called "crimeware," attack toolkits are bundles of malware used to facilitate the launch of attacks against networked computers, according to the report. These kits generally include malicious code for exploiting vulnerabilities in multiple applications and technologies, as well as tools to customize, deploy and launch widespread attacks.

Between July 2009 and June 2010, 61 percent of the web-based threat activity detected by Symantec was attributable to such kits, the report states.

"Attack kits are significantly advancing the evolution of cybercrime into a self-sustaining, profitable and increasingly organized economic model worth millions of dollars," the report states. SC Magazine

Full Story :

[http://www.scmagazineus.com/report-toolkits-now-used-in-the-majority-of-cyberattacks/article/194545/?utm\\_source=](http://www.scmagazineus.com/report-toolkits-now-used-in-the-majority-of-cyberattacks/article/194545/?utm_source=)

## • Researchers turn USB cable into attack tool

George Mason researchers demonstrate how to take control of a laptop via a USB-connected smartphone at the Black Hat DC conference.

(Credit: Angelos Stavrou)

Two researchers have figured out a way to attack laptops and smartphones through an innocent-looking USB cable. Cnet Security

Full Story :

[http://news.cnet.com/8301-27080\\_3-20028919-245.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-27080_3-20028919-245.html?part=rss&subj=news&tag=2547-1_3-0-20)

## • Hackers steal \$150,000 with malicious job application

IDG News Service - Small businesses have a new scam to worry about: criminal job applicants who want to hack into online bank accounts.

The U.S. Federal Bureau of Investigation issued a warning Wednesday about a new twist on a long-running computer fraud technique, known as Automated Clearing House fraud.

With ACH fraud, criminals install malicious software on a small business' computer and use it to log into the company's online bank account. They set up bogus fund transfers, adding fake employees or payees, and then move the money offshore. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9205562/Hackers\\_steal\\_150\\_000\\_with\\_malicious\\_job\\_application?source=](http://www.computerworld.com/s/article/9205562/Hackers_steal_150_000_with_malicious_job_application?source=)

# New Vulnerabilities Tested in SecureScout

## • 19092 RTSP Use After Free Vulnerability (MS10-075/2281679) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Windows Media Player Network Sharing Service that could allow a remote user to send a specially crafted network packet to an instance of the application's network streaming service and cause remote code execution in the context of the current application.

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

### References:

\* VUPEN: VUPEN/ADV-2010-2622

<http://www.vupen.com/english/advisories/2010/2622>

\* BID: 43776

<http://www.securityfocus.com/bid/43776>

\* SECTRACK: 1024545

<http://securitytracker.com/alerts/2010/Oct/1024545.html>

\* MS: MS10-075

<http://www.microsoft.com/technet/security/Bulletin/MS10-075.mspx>

### CVE Reference:

CVE-2010-3225 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## • 19093 Comctl32 Heap Overflow Vulnerability (MS10-081/2296011) (Remote File Checking)

A remote code execution vulnerability exists in the way that the Windows common control library renders specially crafted Web sites when using a third-party scalable vector graphics (SVG) viewer. This vulnerability could allow code execution if a user visited a specially crafted Web page. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

#### References:

- \* VUPEN: VUPEN/ADV-2010-2628  
<http://www.vupen.com/english/advisories/2010/2628>
- \* BID: 43717  
<http://www.securityfocus.com/bid/43717>
- \* MS: MS10-081  
<http://www.microsoft.com/technet/security/Bulletin/MS10-081.msp>
- \* SECTRACK: 1024549  
<http://www.securitytracker.com/id?1024549>

#### CVE Reference:

CVE-2010-2746 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19094 Windows Media Player Memory Corruption Vulnerability (MS10-082/2378111) (Remote File Checking)

A remote code execution vulnerability exists in the way that the Windows Media Player deallocates objects during a reload operation via a Web browser. This vulnerability could allow code execution if a user visits a specially crafted Web page. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

#### References:

- \* VUPEN: VUPEN/ADV-2010-2629  
<http://www.vupen.com/english/advisories/2010/2629>
- \* BID: 43772  
<http://www.securityfocus.com/bid/43772>
- \* MS: MS10-082  
<http://www.microsoft.com/technet/security/Bulletin/MS10-082.msp>
- \* SECTRACK: 1024550  
<http://www.securitytracker.com/id?1024550>

#### CVE Reference:

CVE-2010-2745 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19095 LPC Message Buffer Overrun Vulnerability (MS10-084/2360937) (Remote File Checking)

An elevation of privilege vulnerability exists in the Remote Procedure Call Subsystem (RPCSS) running in the context of the NetworkService account, where a local application can use LPC to request that the LPC server connect back to the client using LRPC. This request could contain specially crafted data designed to cause a stack-based buffer overflow, allowing an authenticated user to access resources running in the context of the NetworkService account.

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

#### References:

- \* VUPEN: VUPEN/ADV-2010-2631  
<http://www.vupen.com/english/advisories/2010/2631>
- \* BID: 43777  
<http://www.securityfocus.com/bid/43777>
- \* MS: MS10-084  
<http://www.microsoft.com/technet/security/Bulletin/MS10-084.msp>
- \* SECTRACK: 1024553  
<http://www.securitytracker.com/id?1024553>

#### CVE Reference:

CVE-2010-3222 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19142 COM Validation Vulnerability (Microsoft Office Word) (MS10-036/983235) (Remote File Checking)

A remote code execution vulnerability exists in the way that affected Microsoft Office software validates COM object instantiation. 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.

This TC checks for the vulnerability specifically in Microsoft Office Word.

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

#### References:

- \* VUPEN: VUPEN/ADV-2010-1393  
<http://www.vupen.com/english/advisories/2010/1393>
- \* SECTRACK: 1024073  
<http://securitytracker.com/alerts/2010/Jun/1024073.html>
- \* MS: MS10-036  
<http://www.microsoft.com/technet/security/bulletin/ms10-036.mspx>
- \* MS: MS10-083  
<http://www.microsoft.com/technet/security/Bulletin/MS10-083.mspx>
- \* CERT: TA10-159B  
<http://www.us-cert.gov/cas/techalerts/TA10-159B.html>
- \* BID: 40574  
<http://www.securityfocus.com/bid/40574>
- \* OVAL: oval:org.mitre.oval:def:7286  
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7286>
- \* SECTRACK: 1024555  
<http://www.securitytracker.com/id?1024555>

#### CVE Reference:

CVE-2010-1263 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19145 UAG Redirection Spoofing Vulnerability (MS10-089/2316074) (Remote File Checking)

A spoofing vulnerability exists in Forefront Unified Access Gateway (UAG). The vulnerability could allow spoofing or redirecting of traffic intended for the UAG server if a UAG user clicks a specially crafted link. An attacker could send a specially crafted URL to a user of the UAG server to redirect Web traffic to a malicious site with content similar to the original Web site. By doing so, the attacker could potentially acquire sensitive information, such as the user's credentials.

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

#### References:

- \* MS: MS10-089  
<http://www.microsoft.com/technet/security/Bulletin/MS10-089.mspx>
- \* CERT: TA10-313A  
<http://www.us-cert.gov/cas/techalerts/TA10-313A.html>
- \* BID: 44631  
<http://www.securityfocus.com/bid/44631>
- \* SECTRACK: 1024707  
<http://securitytracker.com/id?1024707>
- \* VUPEN: VUPEN/ADV-2010-2925  
<http://www.vupen.com/english/advisories/2010/2925>

#### CVE Reference:

CVE-2010-2732 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19146 UAG XSS Allows EOP Vulnerability (MS10-089/2316074) (Remote File Checking)

A cross-site scripting (XSS) vulnerability exists in Forefront Unified Access Gateway (UAG) that could allow specially crafted script code to run under the guise of the server. This is a non-persistent cross-site scripting vulnerability that could allow an attacker to issue commands to the UAG server in the context of the targeted user.

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

#### References:

\* BID: 44632  
<http://www.securityfocus.com/bid/44632>  
\* SECTRACK: 1024707  
<http://securitytracker.com/id?1024707>  
\* VUPEN: VUPEN/ADV-2010-2925  
<http://www.vupen.com/english/advisories/2010/2925>  
\* MS: MS10-089  
<http://www.microsoft.com/technet/security/Bulletin/MS10-089.msp>  
\* CERT: TA10-313A  
<http://www.us-cert.gov/cas/techalerts/TA10-313A.html>

**CVE Reference:**

CVE-2010-2733 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **19147 XSS Issue on UAG Mobile Portal Website in Forefront Unified Access Gateway Vulnerability (MS10-089/2316074) (Remote File Checking)**

A cross-site scripting (XSS) vulnerability exists in Forefront Unified Access Gateway (UAG) that could allow specially crafted script code to run under the guise of the server. This is a non-persistent cross-site scripting vulnerability that could allow an attacker to issue commands to the UAG server in the context of the targeted user.

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

**References:**

\* BID: 44633  
<http://www.securityfocus.com/bid/44633>  
\* SECTRACK: 1024707  
<http://securitytracker.com/id?1024707>  
\* VUPEN: VUPEN/ADV-2010-2925  
<http://www.vupen.com/english/advisories/2010/2925>  
\* MS: MS10-089  
<http://www.microsoft.com/technet/security/Bulletin/MS10-089.msp>  
\* CERT: TA10-313A  
<http://www.us-cert.gov/cas/techalerts/TA10-313A.html>

**CVE Reference:**

CVE-2010-2734 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **19148 XSS in Signurl.asp Vulnerability (MS10-089/2316074) (Remote File Checking)**

A cross-site scripting (XSS) vulnerability exists in Forefront Unified Access Gateway (UAG) that could allow specially crafted script code to run under the guise of the server. This is a non-persistent cross-site scripting vulnerability that could allow an attacker to issue commands to the UAG server in the context of the targeted user.

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

**References:**

\* BID: 44634  
<http://www.securityfocus.com/bid/44634>  
\* SECTRACK: 1024707  
<http://securitytracker.com/id?1024707>  
\* VUPEN: VUPEN/ADV-2010-2925  
<http://www.vupen.com/english/advisories/2010/2925>  
\* MS: MS10-089  
<http://www.microsoft.com/technet/security/Bulletin/MS10-089.msp>  
\* CERT: TA10-313A  
<http://www.us-cert.gov/cas/techalerts/TA10-313A.html>

**CVE Reference:**

CVE-2010-3936 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **19149 Exchange Server Infinite Loop Vulnerability (MS10-106/2407132) (Remote File Checking)**

A denial of service vulnerability exists in the way that the Microsoft Exchange store processes specially crafted RPC calls. The vulnerable code path is only accessible to authenticated users. An authenticated attacker could exploit the vulnerability by sending a specially crafted network message to a computer running the Exchange service. An attacker who successfully exploited this vulnerability could cause the Exchange service to stop responding until manually restarted.

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

## References:

- \* BID: 45297  
<http://www.securityfocus.com/bid/45297>
- \* VUPEN: VUPEN/ADV-2010-3228  
<http://www.vupen.com/english/advisories/2010/3228>
- \* MS: MS10-106  
<http://www.microsoft.com/technet/security/Bulletin/MS10-106.msp>
- \* CERT: TA10-348A  
<http://www.us-cert.gov/cas/techalerts/TA10-348A.html>
- \* SECTRACK: 1024888  
<http://www.securitytracker.com/id?1024888>

## CVE Reference:

CVE-2010-3937 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

### • CVE-2010-3510 Oracle CVSS 2.0 Score = 10.0

Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 9.0, 9.1, 9.2.3, 10.0.2, 10.3.2, and 10.3.3 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Node Manager.

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

#### References:

CONFIRM: <http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html>

CVE Reference: [CVE-2010-3510](http://cve.mitre.org/cve/2010/3510)

### • CVE-2010-3599 Oracle CVSS 2.0 Score = 9.4

Unspecified vulnerability in the Oracle Document Capture component in Oracle Fusion Middleware 10.1.3.4 and 10.1.3.5 allows remote attackers to affect integrity and availability via unknown vectors related to Import Server.

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

#### References:

CONFIRM: <http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html>

CVE Reference: [CVE-2010-3599](http://cve.mitre.org/cve/2010/3599)

### • CVE-2010-3591 Oracle CVSS 2.0 Score = 9.3

Unspecified vulnerability in the Oracle Document Capture component in Oracle Fusion Middleware 10.1.3.4 and 10.1.3.5 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Internal Operations.

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

#### References:

CONFIRM: <http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html>

CVE Reference: [CVE-2010-3591](http://cve.mitre.org/cve/2010/3591)

### • CVE-2010-3592 Oracle CVSS 2.0 Score = 8.5

Unspecified vulnerability in the Oracle Document Capture component in Oracle Fusion Middleware 10.1.3.4 and 10.1.3.5 allows remote attackers to affect integrity and availability via unknown vectors related to Internal Operations.

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

#### References:

CONFIRM: <http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html>

CVE Reference: [CVE-2010-3592](http://cve.mitre.org/cve/2010/3592)

### • CVE-2010-3595 Oracle CVSS 2.0 Score = 7.8

Unspecified vulnerability in the Oracle Document Capture component in Oracle Fusion Middleware 10.1.3.4 and 10.1.3.5 allows remote attackers to affect confidentiality via unknown vectors related to Import Server.

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

**References:**

CONFIRM: <http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html>

**CVE Reference:** [CVE-2010-3595](#)

• **CVE-2010-3593 Oracle CVSS 2.0 Score = 7.5**

Unspecified vulnerability in the Health Sciences - Oracle Argus Safety component in Oracle Industry Applications 5.0, 5.0.1, 5.0.2, and 5.0.3 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Login and LDAP.

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

**References:**

CONFIRM: <http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html>

**CVE Reference:** [CVE-2010-3593](#)

• **CVE-2010-3600 Oracle CVSS 2.0 Score = 7.5**

Unspecified vulnerability in the Client System Analyzer component in Oracle Database Server 11.1.0.7 and 11.2.0.1 and Enterprise Manager Grid Control 10.2.0.5 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

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

**References:**

CONFIRM: <http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html>

**CVE Reference:** [CVE-2010-3600](#)

• **CVE-2011-0272 HP CVSS 2.0 Score = 10.0**

Unspecified vulnerability in HP LoadRunner 9.52 allows remote attackers to execute arbitrary code via network traffic to TCP port 5001 or 5002, related to the HttpTunnel feature.

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

**References:**

XF: <http://xforce.iss.net/xforce/xfdb/64659>

BID: <http://www.securityfocus.com/bid/45792>

HP: <http://www.securityfocus.com/archive/1/515682>

HP: <http://www.securityfocus.com/archive/1/515682>

SECTRAK: <http://securitytracker.com/id?1024956>

SECUNIA: <http://secunia.com/advisories/42898>

**CVE Reference:** [CVE-2011-0272](#)

**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](mailto: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](mailto: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](mailto:info-scanner@securescout.net)