

## 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

Another large data breach. FBI personnel not good enough at combating cyber threats. Millions lost in fraudulent transfers to China. Software security check inputs.

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

### • PlayStation Network hacked, data on millions at risk

Sony may have sustained the largest cyber intrusion since the Heartland Payment Systems breach, disclosing Tuesday that its PlayStation Network (PSN) was hacked to steal sensitive information belonging to users.

Attackers stole personal data belonging to PSN and Qriocity's users between April 17 and 19, Patrick Seybold, a PlayStation spokesman, said in a blog post Tuesday. Qriocity is Sony's music, games, book and video on-demand service.

Roughly 77 million users are registered with PSN and Qriocity. SC Magazine

Full Story :

[http://www.scmagazineus.com/playstation-network-hacked-data-on-millions-at-risk/article/201540/?utm\\_source=feed](http://www.scmagazineus.com/playstation-network-hacked-data-on-millions-at-risk/article/201540/?utm_source=feed)

### • Audit doubts FBI's ability to combat cyberthreats

While the FBI has had some success in countering the most serious cyberattacks that threaten national security, the agency must bolster information sharing and education to effectively investigate intrusions, according to a government audit released Wednesday. The review from the U.S. Department of Justice (DoJ) inspector general assessed the FBI's ability to investigate and counter national security-related cyber intrusions, such as those carried out by foreign adversaries for intelligence or terrorist purposes.

Assessors interviewed 36 agents at 10 FBI field offices and found that 36 percent lacked the networking and counterintelligence expertise to investigate such cases.

Part of the problem is an FBI policy in which agents are rotated among different departments to promote a variety of work experience, the audit found. Specifically, the strategy has reduced the number of qualified cyber agents to assist with such investigations. SC Magazine

Full Story :

[http://www.scmagazineus.com/audit-doubts-fbis-ability-to-combat-cyberthreats/article/201657/?utm\\_source=feedburn](http://www.scmagazineus.com/audit-doubts-fbis-ability-to-combat-cyberthreats/article/201657/?utm_source=feedburn)

### • **FBI warns of millions lost in fraudulent transfers to China**

The FBI is asking U.S. banks to be on the lookout for large wire transfers being sent to accounts registered to companies located in Chinese port cities near the Russian border.

In a fraud alert posted Thursday, federal authorities said they are investigating 20 cases in which the bank accounts of small and midsize businesses in the United States were hijacked to initiate transfers to the bank accounts belonging to Chinese economic and trade companies based in the Heilongjiang province.

Losses between March 2010 and April of this year have totaled about \$11 million, with attempted losses reaching roughly \$20 million, according to the joint alert issued by the FBI, Internet Crime Complaint Center and Financial Services Information Sharing and Analysis Center (FS-ISAC). SC Magazine

Full Story :

[http://www.scmagazineus.com/fbi-warns-of-millions-lost-in-fraudulent-transfers-to-china/article/201573/?utm\\_source=feedburn](http://www.scmagazineus.com/fbi-warns-of-millions-lost-in-fraudulent-transfers-to-china/article/201573/?utm_source=feedburn)

### • **Security Manager's Journal: Software security comes down to checking inputs**

Computerworld - In my previous column, I described how I found out that my company has some developers writing a new application, which I found out about when they came to me for advice on how to store passwords securely in their database. My advice on authenticating users was to use existing software services, rather than building an inferior duplicate. Subsequently, I've had several conversations with the developers about how to improve the security of their code. Coincidentally, my co-columnist Mathias Thurman has also been dealing with the subject of secure software development.

I've had to get back to basics with our developers. As it turns out, security really is an afterthought in their minds. I was surprised to learn that the developers aren't really familiar with what I consider to be the basic fundamentals of secure coding. I'm not a programmer myself, but I would have expected professional programmers to be more knowledgeable than me. In fact, don't they teach this stuff in college? Evidently not. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9216205/Security\\_Manager\\_s\\_Journal\\_Software\\_security\\_comes\\_down\\_to](http://www.computerworld.com/s/article/9216205/Security_Manager_s_Journal_Software_security_comes_down_to)

## **New Vulnerabilities Tested in SecureScout**

### • **19274 Persist Directory RCE Vulnerability (MS11-022/2489283) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

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

#### **References:**

\* BUGTRAQ: 20110412 ZDI-11-125: Microsoft Office PowerPoint PersistDirectoryEntry Remote Code Execution Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/517482/100/0/threaded>

\* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-11-125>

\* MS: MS11-022

<http://www.microsoft.com/technet/security/Bulletin/MS11-022.msp>

\* BID: 47251

<http://www.securityfocus.com/bid/47251>

\* OSVDB: 71770  
<http://osvdb.org/71770>  
\* SECTRACK: 1025340  
<http://www.securitytracker.com/id?1025340>  
\* VUPEN: ADV-2011-0941  
<http://www.vupen.com/english/advisories/2011/0941>

**CVE Reference:**

CVE-2011-0656 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **19275 OfficeArt Atom RCE Vulnerability (MS11-022/2489283) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

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

**References:**

\* BUGTRAQ: 20110207 ZDI-11-044: Microsoft PowerPoint 2007 OfficeArt Atom Remote Code Execution Vulnerability  
<http://www.securityfocus.com/archive/1/archive/1/516233/100/0/threaded>  
\* MISC:  
<http://dvlabs.tippingpoint.com/blog/2011/02/07/zdi-disclosure-microsoft>  
\* MISC:  
<http://zerodayinitiative.com/advisories/ZDI-11-044/>  
\* MS: MS11-022  
<http://www.microsoft.com/technet/security/Bulletin/MS11-022.mspx>  
\* SECTRACK: 1025340  
<http://www.securitytracker.com/id?1025340>  
\* SECUNIA: 43213  
<http://secunia.com/advisories/43213>  
\* VUPEN: ADV-2011-0941  
<http://www.vupen.com/english/advisories/2011/0941>

**CVE Reference:**

CVE-2011-0976 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **19276 Office Component Insecure Library Loading Vulnerability (MS11-023/2489293) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office handles the loading of DLL 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 impacted than users who operate with administrative user rights.

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

**References:**

\* MISC:  
<http://www.fortiguard.com/advisory/FGA-2011-13.html>  
\* MS: MS11-023  
<http://www.microsoft.com/technet/security/Bulletin/MS11-023.mspx>  
\* BID: 47246  
<http://www.securityfocus.com/bid/47246>  
\* OSVDB: 71767  
<http://osvdb.org/71767>  
\* SECTRACK: 1025343  
<http://www.securitytracker.com/id?1025343>  
\* SECUNIA: 44015  
<http://secunia.com/advisories/44015>  
\* VUPEN: ADV-2011-0942  
<http://www.vupen.com/english/advisories/2011/0942>

**CVE Reference:**

CVE-2011-0107 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## • 19277 Microsoft Office Graphic Object Dereferencing Vulnerability (MS11-023/2489293) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office handles graphic objects when parsing a specially crafted Office 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:

- \* MISC:  
<http://dvlabs.tippingpoint.com/blog/2011/02/07/zdi-disclosure-microsoft>
- \* MISC:  
<http://zerodayinitiative.com/advisories/ZDI-11-043/>
- \* MS: MS11-023  
<http://www.microsoft.com/technet/security/Bulletin/MS11-023.msp>
- \* SECTRACK: 1025343  
<http://www.securitytracker.com/id?1025343>
- \* SECUNIA: 43216  
<http://secunia.com/advisories/43216>
- \* SECUNIA: 44015  
<http://secunia.com/advisories/44015>
- \* VUPEN: ADV-2011-0942  
<http://www.vupen.com/english/advisories/2011/0942>

### CVE Reference:

CVE-2011-0977 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## • 19278 Win32k Use After Free Vulnerability (CVE-2011-0662) (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: 47194  
<http://www.securityfocus.com/bid/47194>
- \* OSVDB: 71740  
<http://osvdb.org/71740>
- \* 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-var1-priv-escalation(66395)  
<http://xforce.iss.net/xforce/xfdb/66395>

### CVE Reference:

CVE-2011-0662 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## • 19279 Win32k Use After Free Vulnerability (CVE-2011-0665) (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: 47202

<http://www.securityfocus.com/bid/47202>

\* OSVDB: 71741

<http://osvdb.org/71741>

\* 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-var2-priv-escalation(66396)

<http://xforce.iss.net/xforce/xfdb/66396>

## CVE Reference:

CVE-2011-0665 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19280 Win32k Use After Free Vulnerability (CVE-2011-0666) (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: 47203

<http://www.securityfocus.com/bid/47203>

\* OSVDB: 71742

<http://osvdb.org/71742>

\* 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-var3-priv-escalation(66397)

<http://xforce.iss.net/xforce/xfdb/66397>

## CVE Reference:

CVE-2011-0666 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 19281 Win32k Use After Free Vulnerability (CVE-2011-0667) (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: 47204  
<http://www.securityfocus.com/bid/47204>  
\* OSVDB: 71743  
<http://osvdb.org/71743>  
\* 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-var4-priv-escalation(66398)  
<http://xforce.iss.net/xforce/xfdb/66398>

#### CVE Reference:

CVE-2011-0667 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19282 Win32k Use After Free Vulnerability (CVE-2011-0670) (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: 47205  
<http://www.securityfocus.com/bid/47205>  
\* OSVDB: 71744  
<http://osvdb.org/71744>  
\* 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-var5-priv-escalation(66399)  
<http://xforce.iss.net/xforce/xfdb/66399>

#### CVE Reference:

CVE-2011-0670 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19283 Win32k Use After Free Vulnerability (CVE-2011-0671) (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: 47206  
<http://www.securityfocus.com/bid/47206>  
\* OSVDB: 71745

<http://osvdb.org/71745>

\* 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-var6-priv-escalation(66400)

<http://xforce.iss.net/xforce/xfdb/66400>

#### **CVE Reference:**

CVE-2011-0671 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## **New Vulnerabilities found this Week**

### **• CVE-2011-1725 HP CVSS 2.0 Score = 5.0**

Unspecified vulnerability in HP Network Automation 7.2x, 7.5x, 7.6x, 9.0, and 9.10 allows remote attackers to obtain sensitive information via unknown vectors.

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

#### **References:**

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02789514>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02789514>

**CVE Reference:** [CVE-2011-1725](http://cve.mitre.org/cve/2011/1725)

### **• CVE-2011-1839 IBM CVSS 2.0 Score = 5.0**

IBM Rational Build Forge 7.1.0 uses the HTTP GET method during redirection from the authentication servlet to a PHP script, which makes it easier for context-dependent attackers to discover session IDs by reading (1) web-server access logs, (2) web-server Referer logs, or (3) the browser history.

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

#### **References:**

XF: <http://xforce.iss.net/xforce/xfdb/66714>

VUPEN: <http://www.vupen.com/english/advisories/2011/0919>

AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=swg1PM29655>

**CVE Reference:** [CVE-2011-1839](http://cve.mitre.org/cve/2011/1839)

### **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)